FortiAuthenticator - Two-Factor Authentication Agent for Windows

VERSION 1.0

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

05/10/2015

FortiAuthenticator 4.0 - Two-Factor Authentication Agent for Windows

23-330-264235-20150901

TABLE OF CONTENTS

Change Log

Date	Change Description
2013-10-11	Initial release.
2012-04-03	Update to FortiAuthenticator 1.0 MR3. Added FortiMail, FortiWeb, Citrix Access Gateway
2012-06-20	Update to include challenge-response authentication method for FortiGate and Cisco IOS
2012-09-21	Update to add Cisco IOS
2012-11-01	Update document template
2012-12-05	Add F5 Big-IP Configuration
2013-10-24	Update for FortiAuthenticator 3.0

Introduction

This document has been produced to aid the configuration of the FortiAuthenticator Secure Authentication system with Fortinet solutions and other third party products.

Software versions

Testing was performed with the following versions of software where applicable:

- FortiAuthenticator 3.0
- FortiGate 5.0 GA PR4
- FortiWeb 4.0 MR3 PR6
- FortiClient Connect 4.0 MR3
- FortiManager 4.0 MR3
- Ubuntu 11.04
- OpenSSH version 5.8p1
- Apache version 2.2.17
- Citrix Access Gateway 5.0

Basic Configuration of the FortiAuthenticator

The Basic configuration of the FortiAuthenticator is shown below. Any deviations or change which are required from this configuration will be detailed in the relevant section.

For more details on the setup and configuration of the FortiAuthenticator see the Administration Guide at http://docs.fortinet.com/fortiauthenticator/admin-guides.

Basic Configuration

On first boot, the FortiAuthenticator is configured to the default settings:

```
Port 1 IP: 192.168.1.99
Port 1 Netmask: 255.255.255.0
Default Gateway: 192.168.1.1
```

These setting can be modified by configuring a PC to an address on the same subnet and accessing the Web GUI via https://192.168.1.99/, alternatively you can use the CLI method below.

Configuration Using the CLI

Basic configuration of the interface IP and gateway address can be done using the Command

Line Interface (CLI).

Connect the Management Computer to the FortiAuthenticator unit using the supplied Console Cable

Using a suitable terminal emulation program connect to the unit with the following settings:

```
Baud Rate: 9600
Data Bits: 8
Parity: None
Stop Bits: 1
Flow Control: None
```

Log in to the FortiAuthenticator unit using the default credentials below:

```
Username: admin
Password: <blank>
```

Configure the network settings as required, for example:

```
set port1-ip 10.1.1.99/24
set default-gw 10.1.1.1
```

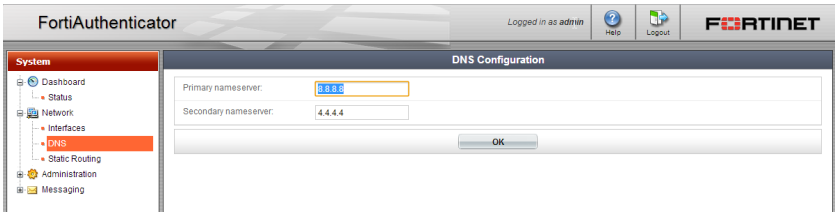
This will give you access to the GUI via the specified IP address, in this case https://10.1.1.99

System Settings

Once the basic networking has been configured, further configuration can be performed via the GUI.

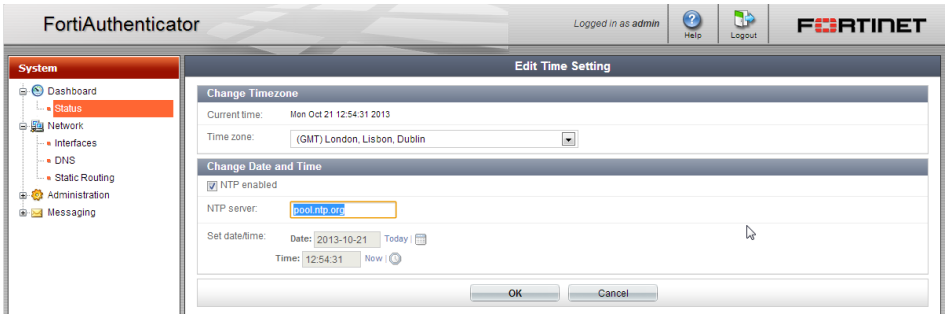
DNS

To enable resolution of the FortiGuard network and other systems such as NTP servers, set your DNS to you local or ISP *nameserver* configuration via *System* > *Network* > *DNS*.



Time Synchronization

FortiToken two-factor authentication uses a time based algorithm to generate Token PINs for use in the authentication process. It is therefore essential that the time is accurate on the FortiAuthenticator system and NTP time synchronization is recommended. Change your settings to a local NTP server for accurate timing via *Dashboard* > *Status* > *System Time* and select *Change*.

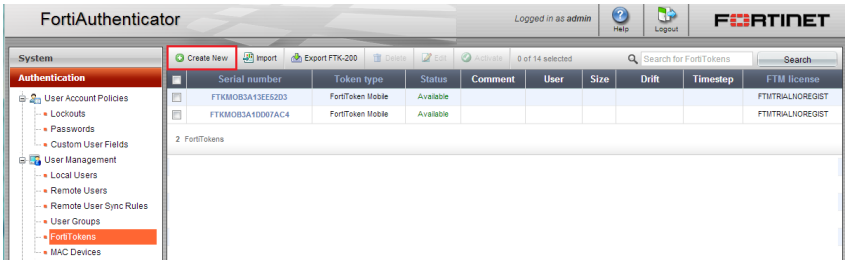


Create a test token

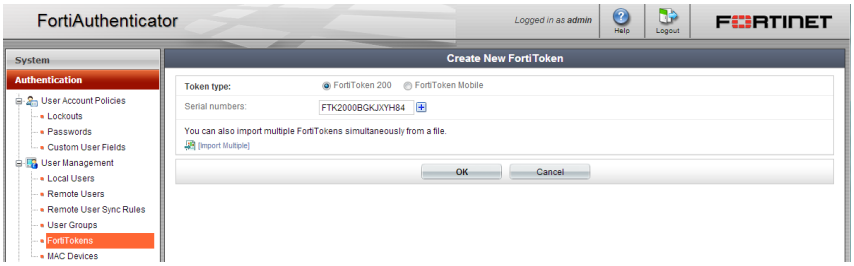
To test two-factor authentication a FortiToken will be required. The token serial can be found on the reverse of the token.

For security reasons a token can only be automatically registered from the FortiGuard network a single time. Should you require to re-register it a subsequent time, you should contact Fortinet support. If you require to use a token on multiple FortiGates, a FortiAuthenticator is recommended.

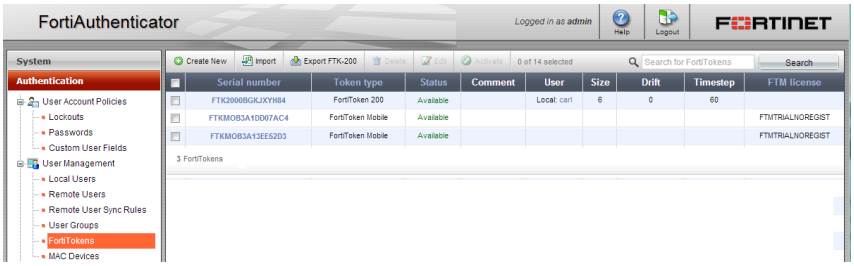
By default, each new installation comes with 2 FortiToken Mobile Tokens included. To register a new physical token (FTK200) go to *Authentication* > *User Management* > *FortiTokens* and select *Create New*.



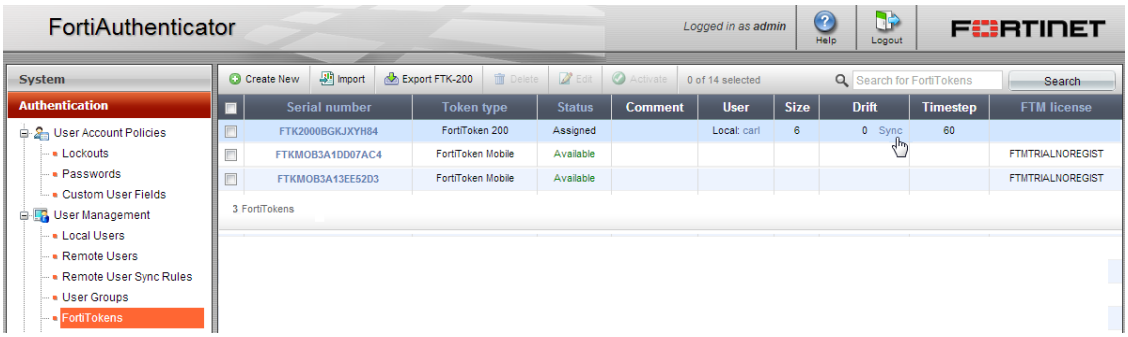
For single tokens, enter the token serial in the *Serial numbers* dialogue box. To register multiple tokens, select the  .



Once registered the token should show as status *Available* in the *Authentication* > *User Management* > *FortiTokens* page.



When new, all tokens are set to a drift of 0 which is a measure of how close the time on the token and time on the FortiAuthenticator match. When new, this should be 0. If you are unable to authenticate at any time, this may be due to clock drift. To force a token drift synchronization, hover the mouse over the drift section for the token and click the *Sync* option which is displayed.



You will be prompted to enter two consecutive PINs from the token. Ensure you have not just used the number for an authentication attempt; if so, wait until the next number refreshed. Once synchronized wait until the next refresh before attempting to authenticate (token PINs are for one-time use, regardless of what they are used for).

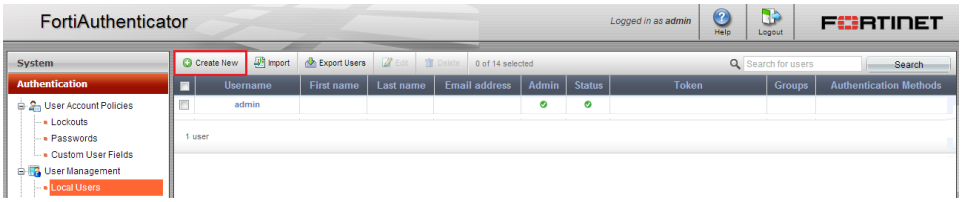
Create test user

For the purpose of this interoperability test, a single user will be created:

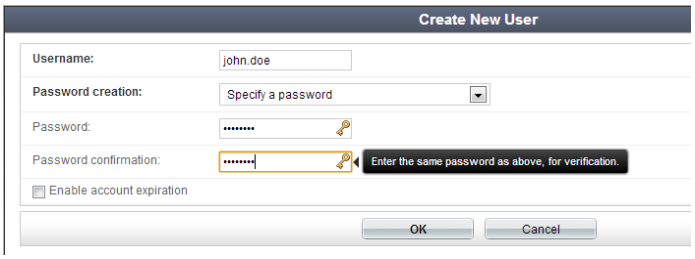
`john.doe`

Test user with RADIUS based username / password and FortiToken.

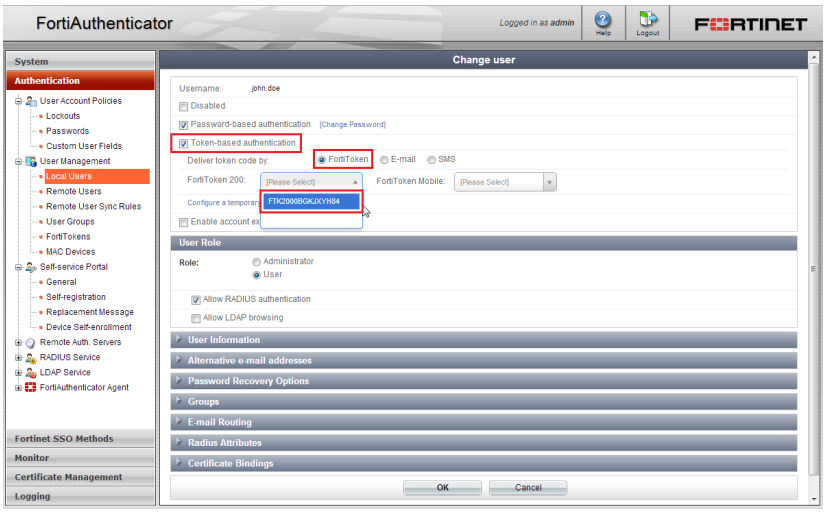
In *Authentication* > *User Management* > *Local Users* select *Create New*.



In the resulting dialogue, enter a username and password for this test user account.

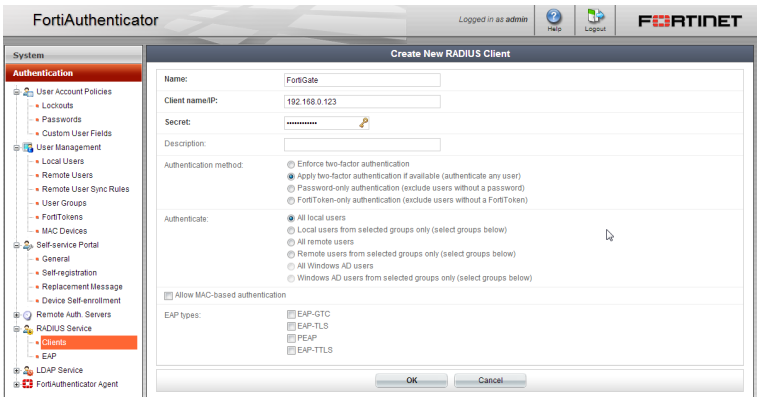


Once created, you will be provided with additional options to edit for the user. For the purpose of this document, all that is needed is to enable *Two-factor authentication* by ticking the radio buttons and select the token serial you have just created from the drop down menu.



Configure a RADIUS Client

Before any device can connect to the FortiAuthenticator to authenticate users via RADIUS, it must be configured as a RADIUS Client. For security reasons, until this is done, the FortiAuthenticator will ignore all authentication requests. In *Authentication* > *RADIUS Service* > *Clients*, select *Create New* and on the resulting page, enter the details of the device you wish to authenticate.



Enter a unique name for the device and the IP from which it will be connecting. Note that this is the IP address of the device itself, not the IP that the users will be authenticating from.

In the secret section, enter a secret password which will be used by both ends of the RADIUS connection to secure the authentication process.

You will have to repeat this process for every device you wish to authenticate against the FortiAuthenticator.

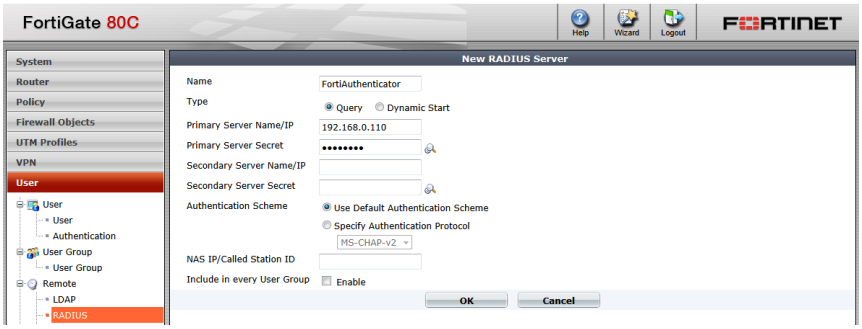
FortiGate

Before proceeding, ensure that you have followed the steps detailed in Basic Configuration. Pay particularly attention to Configure a RADIUS Client and ensure you have created a NAS entry for the device you will be testing otherwise all authentication attempts will be ignored for security reasons.

The FortiGate appliance is the Gateway to your network therefore securing remote access, whether to the box itself (administration or to the network behind it (VPN) is critical. FortiOS versions 4.0 MR3 and above support two factor authentication using FortiToken, however to perform two factor authentication to multiple FortiGate or to versions 4.0 MR2 and lower, you will want to use FortiAuthenticator to enable strong authentication.

Create Remote RADIUS Connection

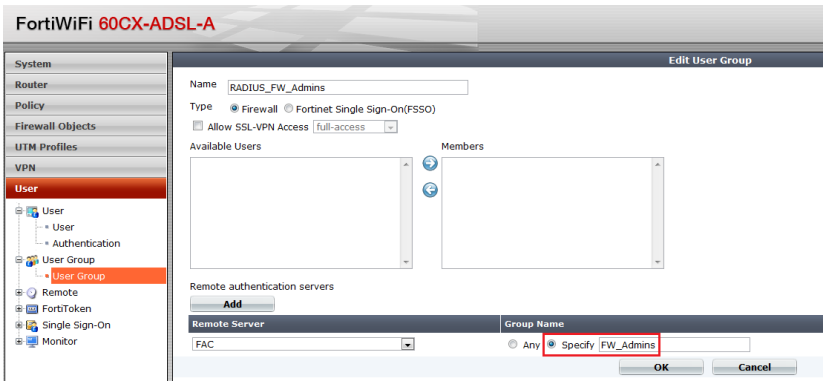
A RADIUS association is required for all FortiGate configurations described below so configure the system to point at the FortiAuthenticator. In *User* > *Remote* > *RADIUS* select *Create New* and configure the details of the FortiAuthenticator. Enter the shared secret which you created previously.



Authenticating Administration Users

Create User Group

On FortiAuthenticator, in *User* > *User Group*, select *Create New*. Create a group called *RADIUS_Admins*,set type to *Firewall* and under *Remote Authentication Servers* select *Add*. Select *FortiAuthenticator* from the drop down list and select *OK* to save.



Do not add any local user to this policy under Available Users. If you do this, RADIUS Authentication will fail.

By specifying the Group Name as shown, FortiGate will only accept authentication for users who are member of the specified group.

Create Admin User

In *System* > *Admin* > *Administrators*, select *Create New*. In the resulting page, enter

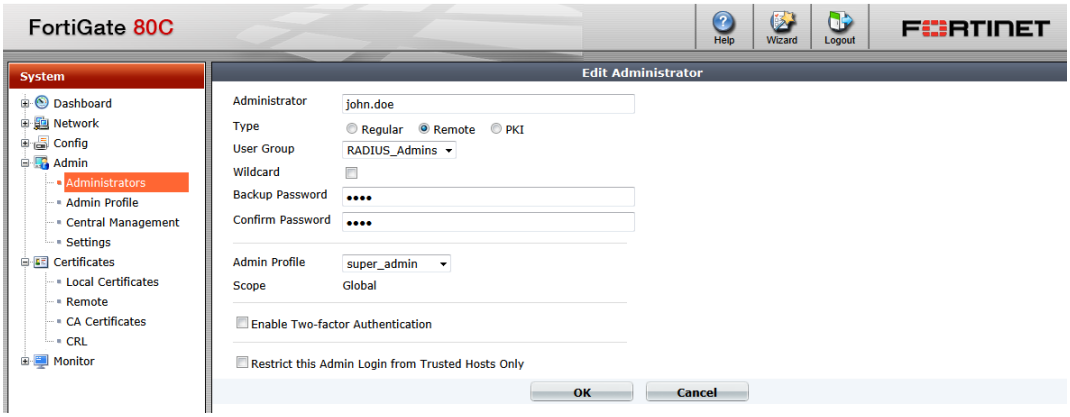
Administrator: `john.doe`

Type: `Remote`

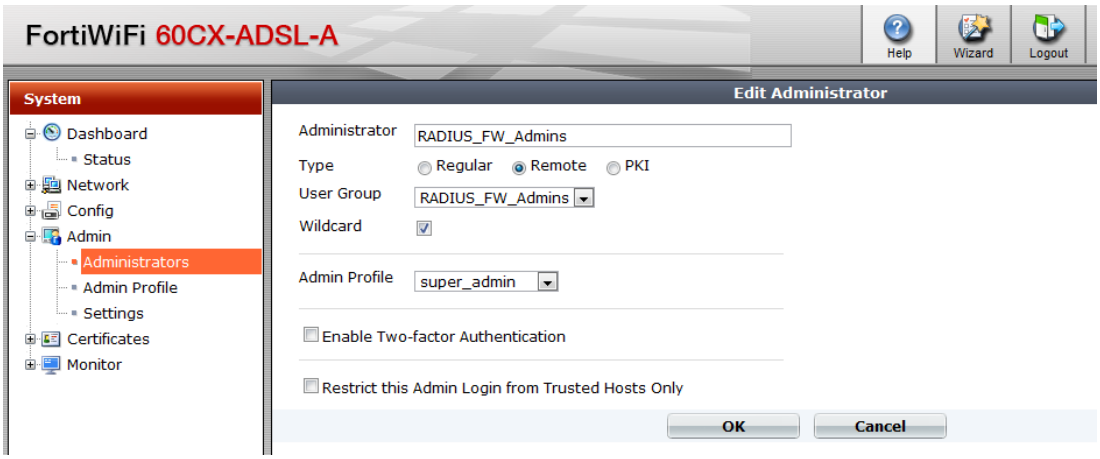
User Group: `RADIUS_Admins`

Admin Profile: `super_admin`

You will also need to enter a backup password which can be used in the event that the RADIUS authentication is unavailable e.g. due to connectivity issues.



There is also the ability to use wildcard accounts to avoid the need to specify each user locally. If this option is enabled, any user from the specified group (or from the whole RADIUS Server if a group is not specified) will be able to authenticate. If this is required, create a new administrator with a name with a descriptive name (it will not be used to authenticate). When the wildcard option is selected, any user configured on the FortiAuthenticator who is in an allowed group will be able to authenticate.



In FortiOS 5.0.4, when wildcard users are configured the challenge response method is not supported, only token appended. This will be resolved in a future release.

Do not select two-factor authentication at this point. The Two Factor Authentication is done externally, so the FortiGate does not need to know it is happening. This is why the FortiAuthenticator is capable of authenticating FortiOS 4.2 and below and third party systems which have no direct support for two-factor authentication.

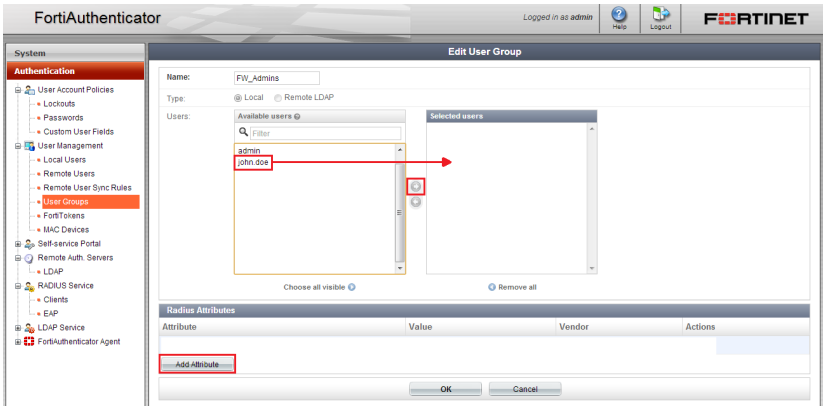
FortiAuthenticator Groups

If a Group Name was specified in the FortiGate configuration, for a user to correctly match the policy and be authenticated, a Fortinet VSA (Vendor Specific Attribute) must be configured on FortiAuthenticator. RADIUS Attributes are sent in the Access-Accept packet and can be configured at the group or user level.

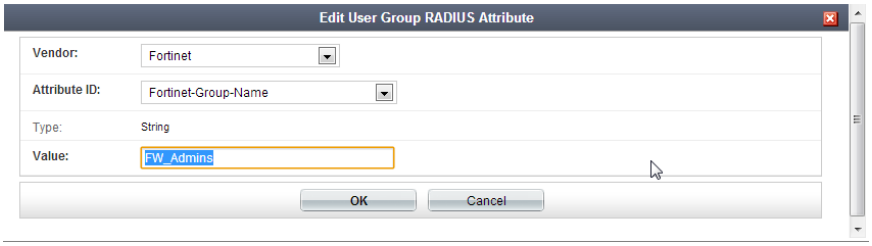
In this example, a group called FW_Admins is going to be created, containing the user john.doe with the Fortinet-Group-Name Attribute value of FW_Admins.

On FortiAuthenticator, browse to *Authentication* > *User Management* > *User Groups* and select *Create New*.

Create a new group named FW_Admins, select the user and click the right arrow to move them into the Selected Users.



Next, select *Add Attribute* and add the *Fortinet-Group-Name* Attribute with the value of *FW_Admins* and select *OK*.

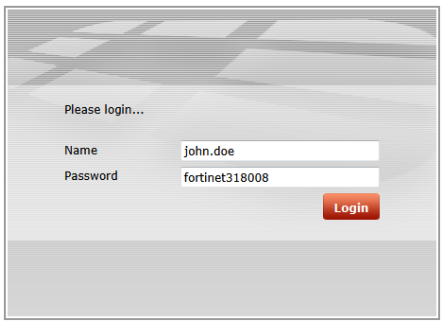


Log out of the FortiGate and log back into the FortiGate Admin GUI with your new credentials. The Username and Password used to authenticate will include the 6-digit two-factor authentication PIN from your token:

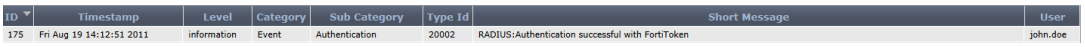
Username: `john.doe`

Password: `<password><Token PIN>`

For example, if the password was *fortinet* and one-time PIN was *318008*, the login would become



Successful authentication will provide the user with access to the device and will generate a login event log on the FortiAuthenticator.



If authentication is unsuccessful, follow the steps in the Chapter Appendix A – Debugging to identify what is wrong.

RADIUS Packets

The following shows the RADIUS Packet decodes for the Access-Request from the FOrtiGate and the Access-Accept from the FortiAuthenticator. The returned groups information that allows the user privilege to be set is displayed in the Fortinet VSA as Fortinet-Group-Name = FW_Admins.

```
Radius Protocol
    Code: Access-Request (1)
    Packet identifier: 0xb (11)
    Length: 101
    Authenticator: 824bb2ccfed9bfec82032ea8243dec0b
    [The response to this request is in frame 2]
  Attribute Value Pairs
    AVP: l=18  t=NAS-Identifier(32): FW60CA3911000454
    AVP: l=10  t=User-Name(1): john.doe
    AVP: l=18  t=User-Password(2): Encrypted
    AVP: l=10  t=Acct-Session-Id(44): 00000007
    AVP: l=13  t=Connect-Info(77): admin-login
    AVP: l=12  t=Vendor-Specific(26) v=Fortinet(12356)
      VSA: l=6 t=Fortinet-Vdom-Name(3): root
```

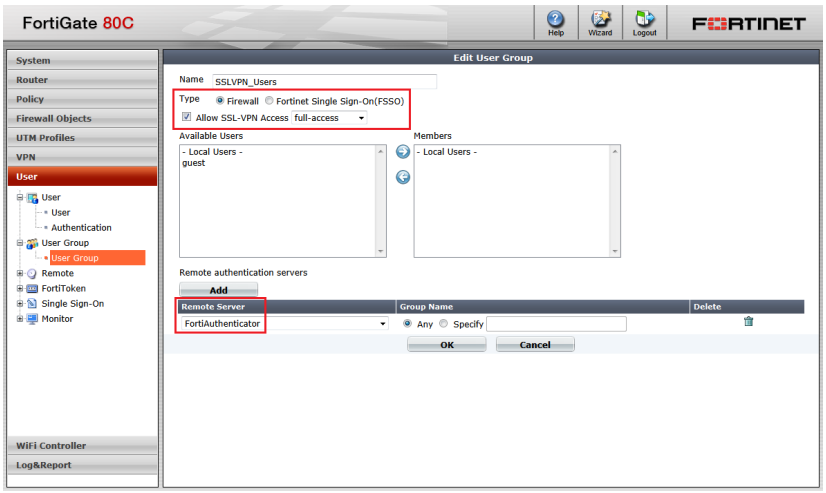
```
Radius Protocol
    Code: Access-Accept (2)
    Packet identifier: 0xb (11)
    Length: 37
    Authenticator: 5e8d8cb60dab8262701502b803f9202a
    [This is a response to a request in frame 1]
    [Time from request: 0.112846000 seconds]
  Attribute Value Pairs
    AVP: l=17  t=Vendor-Specific(26) v=Fortinet(12356)
      VSA: l=11 t=Fortinet-Group-Name(1): FW_Admins
```

Authenticating SSL-VPN Users

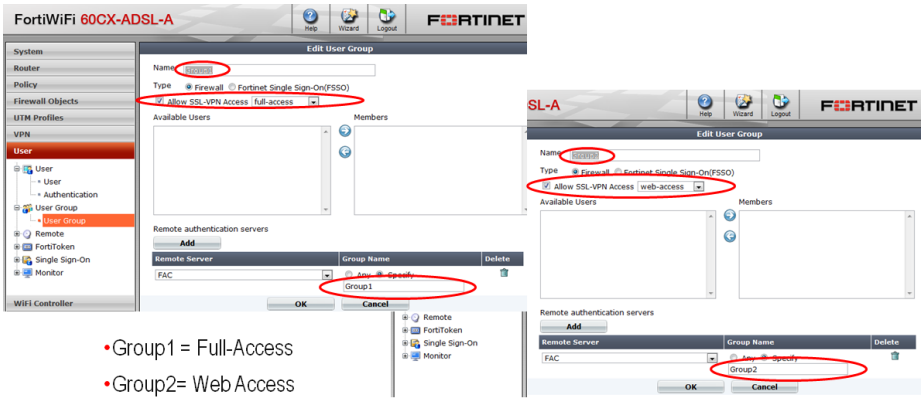
This guide does not detail how to configure the SSL-VPN, only how to enable secure authentication using FortiAuthenticator. For more information on configuring the SSL-VPN please see the SSL-VPN Guide for your specific firmware release here http://docs.fortinet.com/d/fortigate-ssl-vpn-3.

Create User Group

In *User > User Group*, select *Create New*. Create a group called *SSLVPN_Users*, set type to *Firewall* and enable *Allow SSL-VPN Access* with your selected access permissions. Under *Remote Authentication Servers*, select *Add*. Select *FortiAuthenticator* from the drop down list and select *OK* to save.



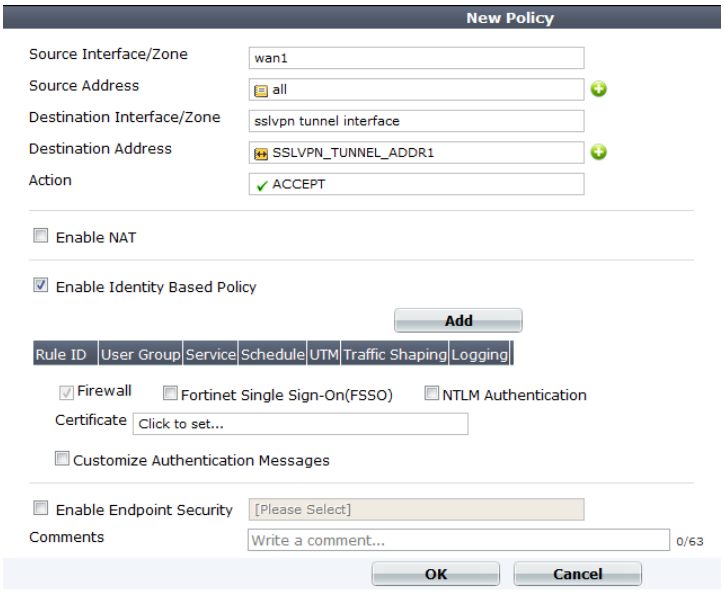
The Group Name configuration can be used to limit which users can authenticate or to limit what they can do in the VPN (by creating multiple groups in conjunction with the Allow SSL-VPN Access option).



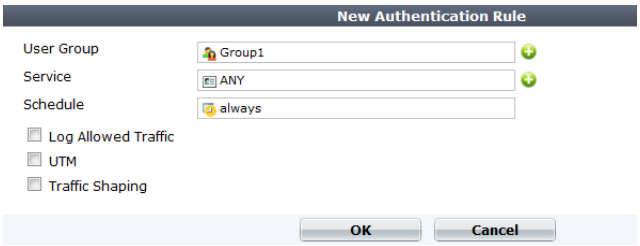
Firewall SSL VPN Policy

Create a firewall policy which enables SSL-VPN access into you chosen network. In this example, a policy is being created from WAN1 to the Internal network for the defined Group.

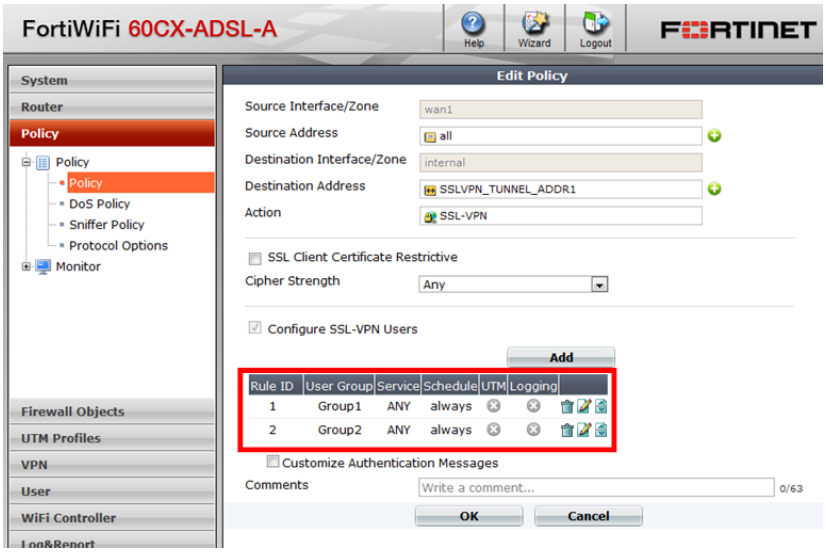
Go to *Policy & Objects* > *Policy* > *IPv4* and select *Create New*. Set *Source Interface* to *WAN1*, *Destination Interface* to *Internal* and *Action* to *SSL-VPN*.



Enable *Identity Based Policy* and add all the user groups allowed to log into the SSL-VPN.



Select the required *Group* from *Available*. Select *Any* from the *Available Services*. Select *OK* and *OK* again on the *Edit Policy* page to save the settings. Where multiple user groups have been configured to allow differentiated VPN access, specify all user groups at this point e.g



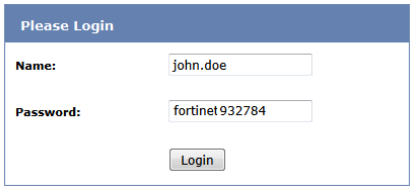
User Login – Password + Token PIN Appended

Attempt to log into the FortiGate SSL-VPN GUI e.g. https://192.168.1.99:10443 (depending upon your settings) with your new credentials. The *Username* and *Password* used to authenticate will include the 6-digit two-factor authentication PIN from your token:

Username: `john.doe`

Password: `<password><Token PIN>`

For example, if the password was *fortinet* and one-time PIN was *318008*, the login would become



Successful authentication will provide the user with access to the VPN-Portal with the configuration specific to your configured user group and will generate a login event log on the FortiAuthenticator

ID	Timestamp	Level	Category	Sub Category	Type Id	Short Message	User
193	Mon Aug 22 09:55:11 2011	information	Event	Authentication	20002	RADIUS:Authentication successful with FortiToken	john.doe

If authentication is unsuccessful, follow the steps in the Chapter Debugging Authentication to identify what is wrong.

User Login – Token PIN Challenge

Whilst the PIN Appended method is the most widely supported method of authentication for 3rd party systems, FortiGate SSL VPN supports the RADIUS Challenge-Response mechanism. This allows the user to enter their username and password and then be challenged separately for the token PIN which is more intuitive. No changes need to be made to the systems to support either method and they can be used interchangeably.

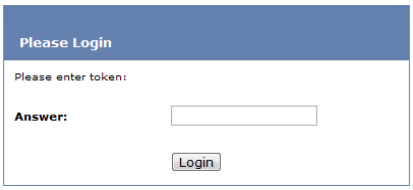
Attempt to log into the FortiGate SSL-VPN GUI e.g. https://192.168.1.99:10443 (dependent on your settings) with your new credentials.

Username: `john.doe`

Password: `<password><Token PIN>`

For example, if the password was *fortinet*, the login would become

The FortiAuthenticator will detect that the password is correct but the token PIN has not been provided and issue a RADIUS Challenge. FortiGate detects this and prompts the user for the additional information.



The user should enter the correct token PIN and select *login*.

Successful authentication will provide the user with access to the VPN-Portal with the configuration specific to your configured user group and will generate a login event log on the FortiAuthenticator

ID	Timestamp	Level	Category	Sub Category	Type Id	Short Message	User
193	Mon Aug 22 09:55:11 2011	information	Event	Authentication	20002	RADIUS:Authentication successful with FortiToken	john.doe

If authentication is unsuccessful, follow the steps in the Chapter Debugging Authentication to identify what is wrong.

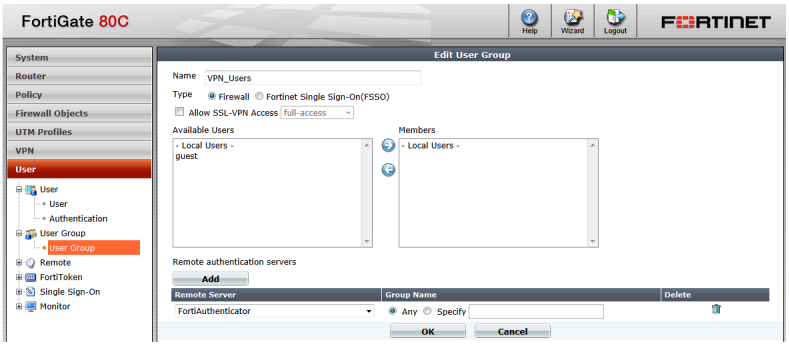
IPSec VPN

Note that this guide does not detail how to configure the IPSec VPN or the FortiClient Connect client, only how to enable secure authentication using FortiAuthenticator. For more information on configuring the VPN on FortiGate and the FortiClient Connect client please see the relevant documentation here http://docs.fortinet.com/fortigate/admin-guides.

This section assumes you have a working IKE configuration.

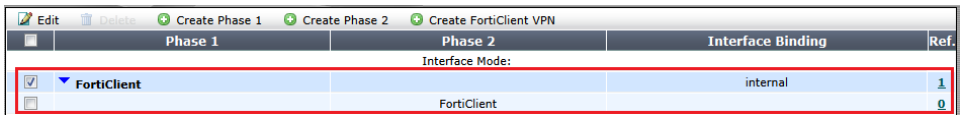
Create User Group

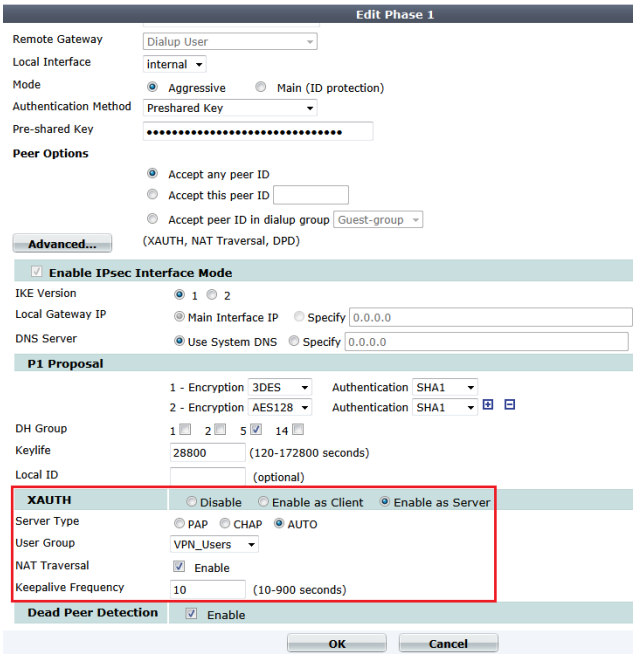
In *User* > *User Group*, select *Create New*. Create a group called *VPN_Users*,set *Type* to *Firewall*, and under *Remote Authentication Servers* select *Add*. Select *FortiAuthenticator* from the drop down list and select *OK* to save.



Edit Existing IKE Policy

To enable FortiAuthenticator strong two-factor authentication, the existing IKE Policy must be configured to enable XAUTH (eXtended AUTHentication). To do this browse to *VPN* > *IPSec* > *Auto Key (IKE)* and edit the *Phase 1* settings of your VPN (select the radio button of the first entry for your VPN and click *Edit*).




Edit Phase 1
Remote Gateway
Dialup User
Local Interface
internal
Mode
Aggressive
Main (ID protection)
Authentication Method
Preshared Key
Pre-shared Key
Peer Options
Accept any peer ID
Accept this peer ID
Accept peer ID in dialup group
Guest-group
Advanced...
(XAUTH, NAT Traversal, DPD)
Enable IPsec Interface Mode
IKE Version
Local Gateway IP
Main Interface IP
Specify
0.0.0.0
DNS Server
Use System DNS
P1 Proposal
1 - Encryption
3DES
Authentication
SHA1
2 - Encryption
AES128
DH Group
Keylife
28800
(120-172800 seconds)
Local ID
(optional)
XAUTH
Disable
Enable as Client
Enable as Server
Server Type
PAP
CHAP
AUTO
User Group
VPN_Users
NAT Traversal
Enable
Keepalive Frequency
10
(10-900 seconds)
Dead Peer Detection
Enable
OK
Cancel

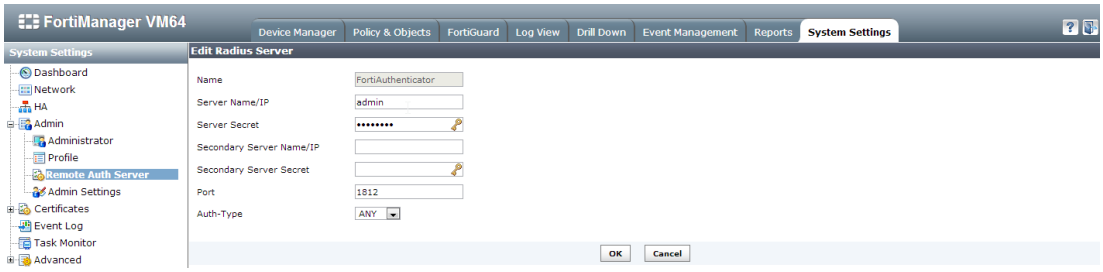
FortiManager

Before proceeding, ensure that you have followed the steps detailed in "Basic Configuration" on page 7. Pay particular attention to "Create test user" on page 11 and ensure you have created a NAS entry for the device you will be testing otherwise all authentication attempts will be ignored for security reasons.

Configure the RADIUS Server

Log into the FortiManager GUI and go to *System Settings* > *Admin* > *Remote Auth Server*. Select *Create New* and *RADIUS*.

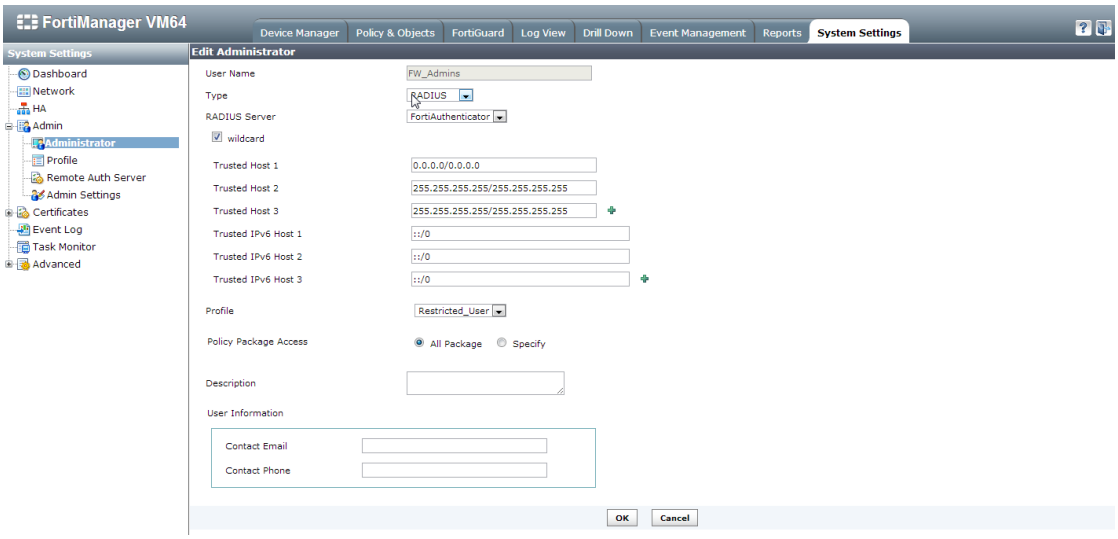
Enter the details of the remote FortiAuthenticator including the shared secret.



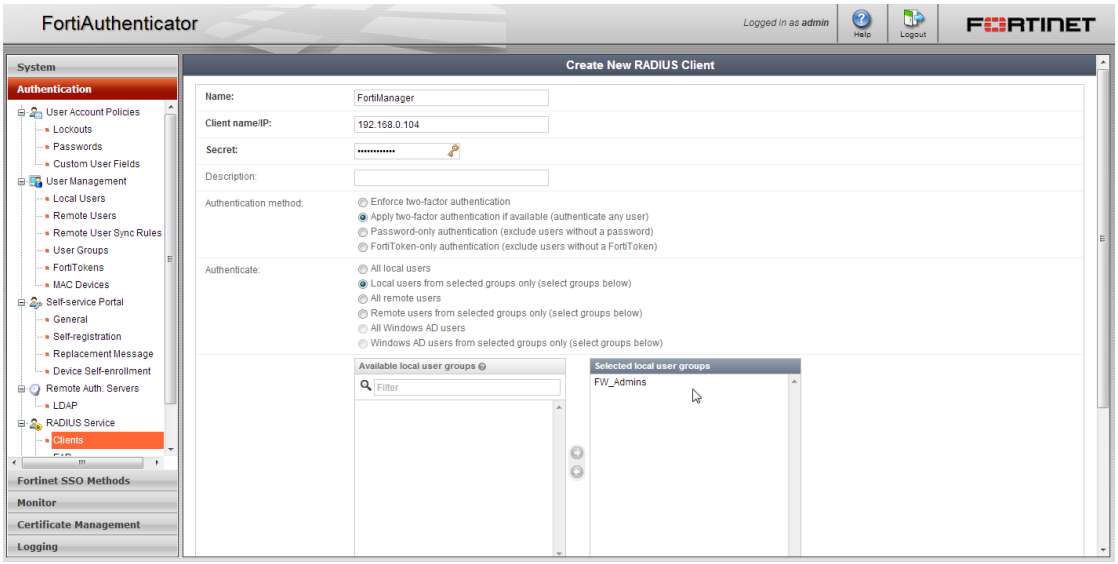
Create the Admin Users

In *System Settings* > *Admin* > *Administrator*, select *Create New*. Enter a name for the config; if this is for a single admin user, enter the user name, if this is for multiple users, enter a generic name and select *Wildcard*.

Select *Auth Type RADIUS* and select the RADIUS server you created in the previous step.



Wildcard authentication will allow authentication from any account on the FortiAuthenticator. To restrict authentication, RADIUS Service Clients can be configured to only authenticate specific user groups.



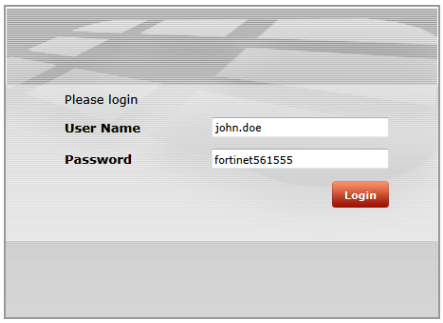
Testing

Attempt to log into the FortiManager GUI with your new credentials. The *Username* and *Password* used to authenticate will include the 6-digit two-factor authentication PIN from your token:

Username: `john.doe`

Password: `<password><Token PIN>`

For example, if the password was *fortinet* and the one-time PIN was *561555*, the login would become



Successful authentication will provide the user with access to the FortiManager and will generate a login event log on the FortiAuthenticator.

ID	Timestamp	Level	Category	Sub Category	Type Id	Short Message	User
193	Mon Aug 22 09:55:11 2011	information	Event	Authentication	20002	RADIUS:Authentication successful with FortiToken	john.doe

If authentication is unsuccessful, follow the steps in Appendix A – Debugging to identify what is wrong.

As of FortiManager 5.0.4, RADIUS Challenge Response is not supported. Only Token Appending is supported. This will be resolved in a future release.

FortiWeb

Before proceeding, ensure that you have followed the steps detailed in Basic Configuration. Pay particular attention to "Create test user" on page 11 and ensure you have created a NAS entry for the device you will be testing otherwise all authentication attempts will be ignored for security reasons.

FortiWeb, (tested to the latest version at the time. 4.0 MR3 PR6) does not support challenge-response so the Token-Appended method should be used.

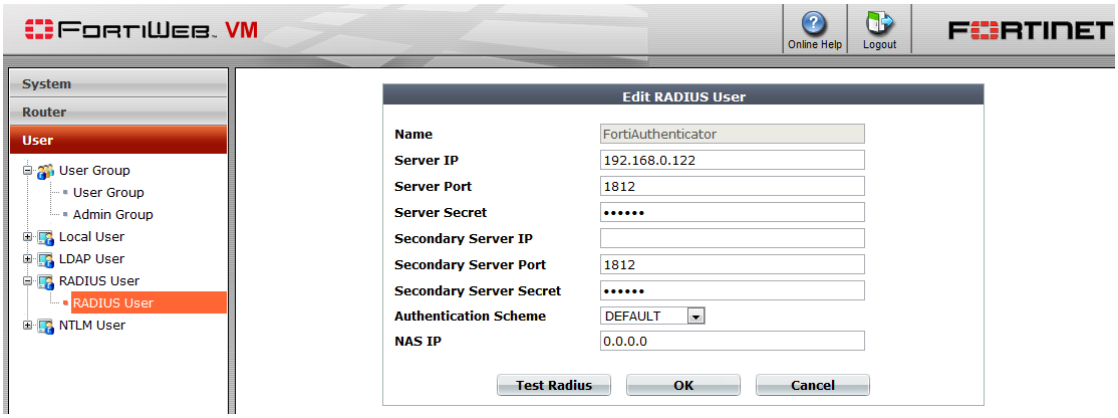
Configure the RADIUS Server

Log into the FortiWeb GUI and go to *User* > *RADIUS User* > *RADIUS User*.

The FortiWeb GUI incorrectly refers to RADIUS User whereas this is actually the RADIUS Server (FortiAuthenticator) configuration. This will be changed in future versions of FortiWeb.

Select *Create New*.

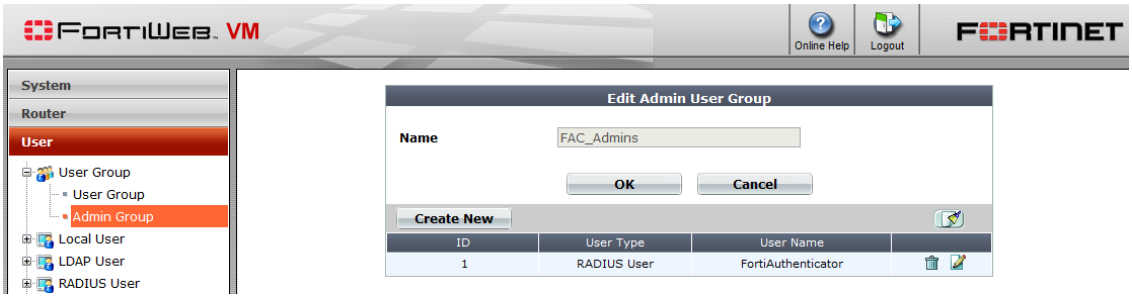
Enter the details of the remote FortiAuthenticator including the shared secret.



Create an Admin Group

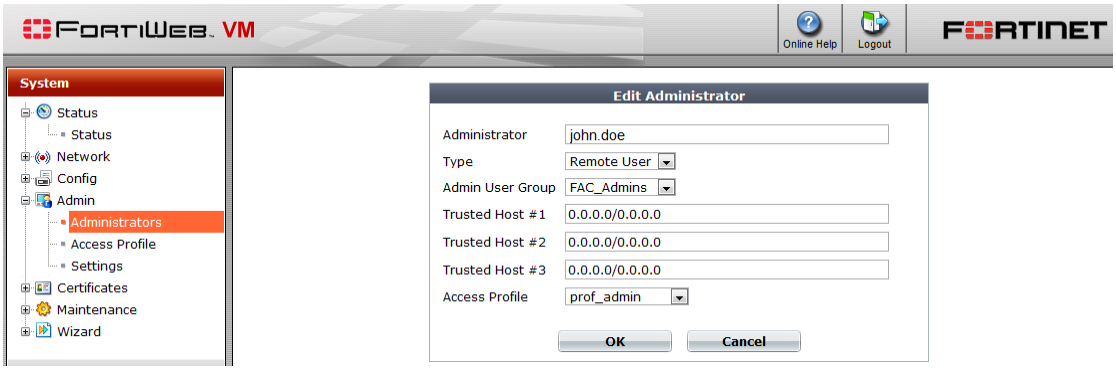
In *User* > *Admin Group*, select *Create New*. Enter the Auth Type RADIUS and select the RADIUS server you created in the previous step under the heading user.

Enter the RADIUS server name at this point, not the User Name. This is an error in the GUI and will be rectified in a later release of the FortiWeb GUI.



Create an Admin User

Go to *System* > *Admin* > *Administrators*, and select *Create New*. Enter the details of the user to be authenticated, set the type to *Remote User*, the *Admin User Group* (as created in the previous step) and select the access profile to use.



FortiWeb does not currently support wildcard users or user groups.

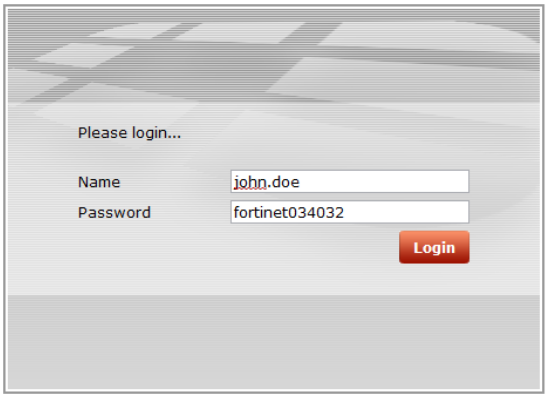
Admin Logon

Attempt to log into the FortiWeb GUI e.g. https://192.168.1.99 (dependent on your settings) with the FortiAuthenticator credentials. The Username and Password used to authenticate will include the 6-digit two-factor authentication PIN from your token:

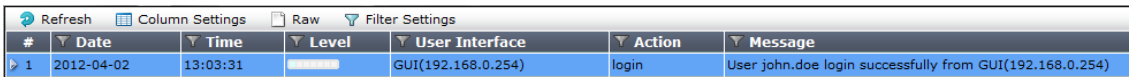
Username:john.doe

Password:<password><Token PIN>

For example, if the password was *fortinet* and the one-time PIN was *034032*, the login would become



Successful authentication will provide the user with access to the FortiWeb and will generate a login event log on the FortiAuthenticator.



If authentication is unsuccessful, follow the steps in the Chapter Debugging Authentication to identify what is wrong.

FortiMail

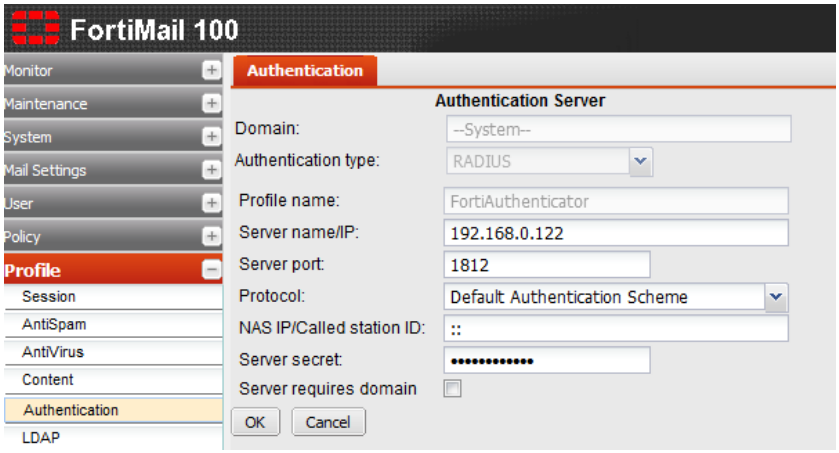
Before proceeding, ensure that you have followed the steps detailed in "Basic Configuration" on page 7. Pay particular attention to "Create test user" on page 11 and ensure you have created a NAS entry for the device you will be testing otherwise all authentication attempts will be ignored for security reasons.

Admin Login

Configure the RADIUS Server

Log into the FortiMail GUI and browse to *Profile* > *Authentication* and select *New*.

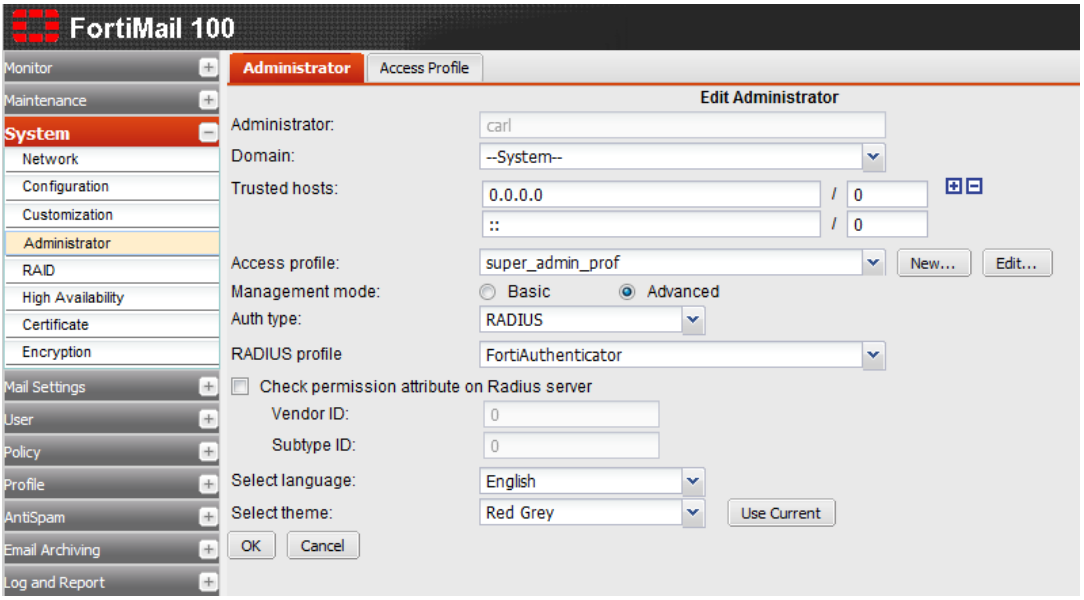
Enter the details of the remote FortiAuthenticator including the FortiAuthenticator IP, Authentication Port (1812), Port, Protocol (authentication scheme) and shared secret.



In *System* > *Administrator*, select *New*. Enter the *User Name*, set *Auth Type* to *RADIUS* and select the RADIUS server you created in the previous step.

FortiMail Administrator configuration does not support the use of wildcard users, i.e. those not defined locally. The use of a wildcard "*" for username will not work here.

Create the Admin User



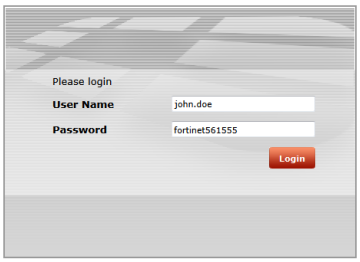
Admin User Logon

Attempt to log into the FortiManager GUI e.g. https://192.168.1.99 (depending upon your settings) with your new credentials. The *Username* and *Password* used to authenticate will include the 6-digit two-factor authentication PIN from your token:

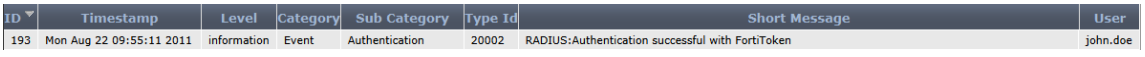
Username: `john.doe`

Password: `<password><Token PIN>`

For example, if the password was *fortinet* and the one-time PIN was *561555*, the login would become



Successful authentication will provide the user with access to the FortiManager and will generate a login event log on the FortiAuthenticator.



ID	Timestamp	Level	Category	Sub Category	Type Id	Short Message	User
193	Mon Aug 22 09:55:11 2011	information	Event	Authentication	20002	RADIUS:Authentication successful with FortiToken	john.doe

If authentication is unsuccessful, follow the steps in the Chapter Debugging Authentication to identify what is wrong.

Cisco IOS based switches and routers

The following was tested with a Cisco 2950 switch running IOS 12.1(13). While this should work with other versions and IOS based routers, the command structure on the Cisco IOS is liable to vary between versions so please consult the Cisco documentation for changes.

Before proceeding, ensure that you have followed the steps detailed in Chapter titled "Basic Configuration" on page 7. Pay particularly attention to "Create test user" on page 11 and ensure you have created a NAS entry for the device you will be testing otherwise all authentication attempts will be ignored for security reasons.

Telnet Authentication

Configure the Cisco switch to allow remote access via Telnet. To do this enter enable mode on the switch and execute to begin editing the configuration:

```
Switch> en
Enter Password: *********
Switch# conf t
Switch(config)#
```

Enter the following commands to enable an IP address on the switch and enable telnet management:

```
Switch(config)# interface Vlan1
Switch(config)# ip address 192.168.0.253 255.255.255.0
Switch(config)# ip default-gateway 192.168.0.1
Switch(config)# no shutdown
```

Enter the following commands to enable two-factor authentication:

```
Switch(config)# aaa new-model
Switch(config)# aaa authentication login default group
radius
Switch(config)# radius-server host 192.168.0.122 auth-port
1812 key fortinet1234
Switch(config)# radius-server retransmit 3
```

Attempt to log in to the switch via telnet and you should be presented with a two-factor enhanced login:

```
telnet 192.168.0.253

User Access Verification

Username: john.doe

Password: fortinet

Please enter token: 721194

Switch>
```

Notice that the login has dropped the user into the non privileged admin level denoted by the >. Enable mode is accessed via the command enable and entering the enable password.

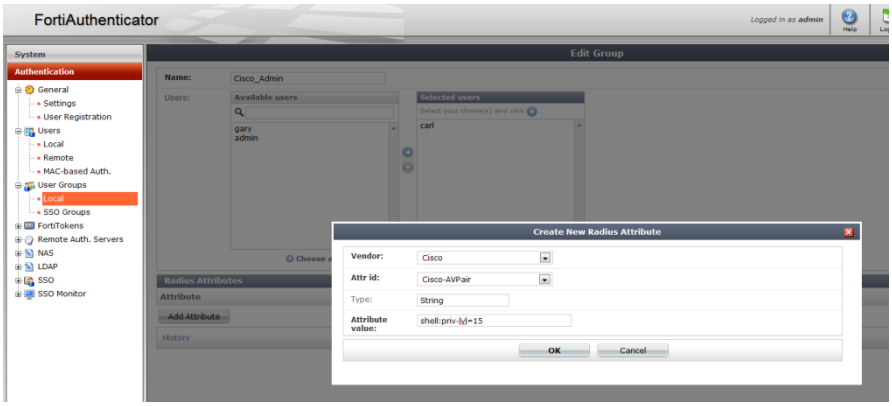
Configure Enable Authorization

To directly authenticate the user into enable mode, it is possible to include an authorization attribute in the RADIUS Access-Accept packet. Cisco uses the following attribute from their standard RADIUS Dictionary for this purpose:

```
Cisco-AVPair = shell:priv-lvl=15
```

RADIUS Attributes can be configured either at the group or user level. The following example sets this attribute at the group level but the configuration mechanism is the same for both.

1. Go to *Authentication* > *User Groups* > *Local* and create a new group called *Cisco_Admins*. Add the required users to this group.
2. Edit the group and select *Add Attributes*.
3. Set vendor to *Cisco* and *Attribute-ID* to *Cisco-AV-Pair*.
4. In the *Attribute Value* field enter *shell:priv-lvl=15* which will give full administrative rights to the user.



Create a second Attribute with *Vendor* set to *Default* (this is the RADIUS RFC standard dictionaries), *Attribute-ID* set to *Service-Type* and *Attribute* set to *Value NAS-Prompt-User*.

To configure the switch to accept these attributes, enter the following configuration:

```
Switch(config)#aaa authorization exec default radius
```

Attempt to login again

```
telnet 192.168.0.253
User Access Verification
Username: john.doe
Password: fortinet
Please enter token: 983403
Switch#
```

Notice that the user is granted the enable (15) privilege level denoted by #.

Privilege Levels

The default Cisco IOS privilege levels are defined as:

Privilege Level	Result
0	Seldom used, but includes five commands: *disable*, *enable*, *exit*, *help*, and *logout*.
1	User level only (prompt is switch>). The default level for login.
15	Privileged level (prompt is router#), the level after going into enable mode

Whilst authorization levels 0, 1, and 15 are configured by default, levels 2 to 14 are undefined and can be used to create additional levels by adding and removing specific CLI commands e.g.

To specify which commands will exist in privilege level 7, issue the following commands on Switch1 from the console:

```
Switch1(config)# privilege configure level 7 snmp-server host
Switch1 (config)# privilege configure level 7 snmp-server enable
Switch1 (config)# privilege configure level 7 snmp-server
Switch1 (config)# privilege exec level 7 ping
Switch1 (config)# privilege exec level 7 configure terminal
Switch1 (config)# privilege exec level 7 configure
```

This level can be then authorized by creating a separate FortiAuthenticator group, including the required users and specifying the new RADIUS Attribute privilege level e.g.

```
Cisco-AVPair = shell:priv-lvl=7
```

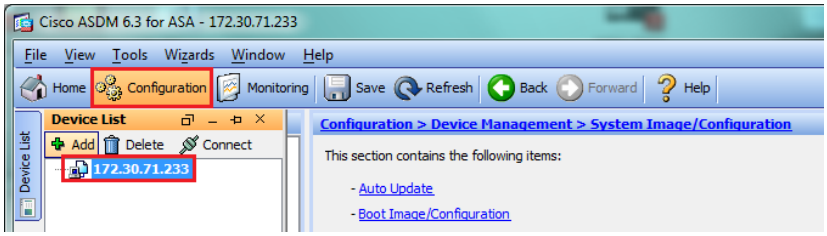
Cisco ASA

The following was tested with a Cisco ASA 5520 running ASA version 8.2(1) and ASDM 6.3(5). Whilst this should work with other ASA versions, Cisco firmware is liable to vary between versions so please consult the Cisco documentation for changes. The configuration of the Cisco ASA device requires the installation of the ASDM management software and/or Oracle Java.

Before proceeding, ensure that you have followed the steps detailed in Chapter titled "Basic Configuration" on page 7. Pay particular attention to "Create test user" on page 11 and ensure you have created a NAS entry for the device you will be testing otherwise all authentication attempts will be ignored for security reasons.

Configuring System Authentication

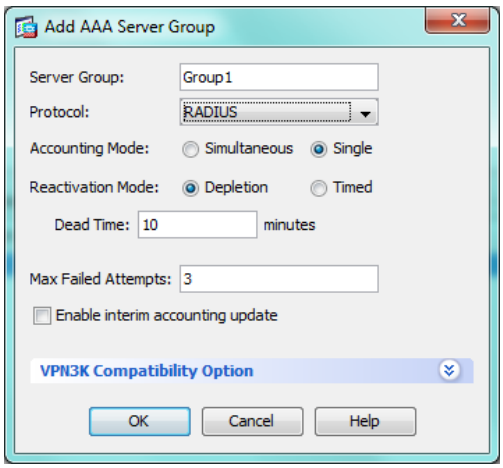
Select the relevant ASA device in *Device List* and then *Configuration* from top menu.



In *Device Management*, go to *Users/AAA* > *AAA Server Groups*.

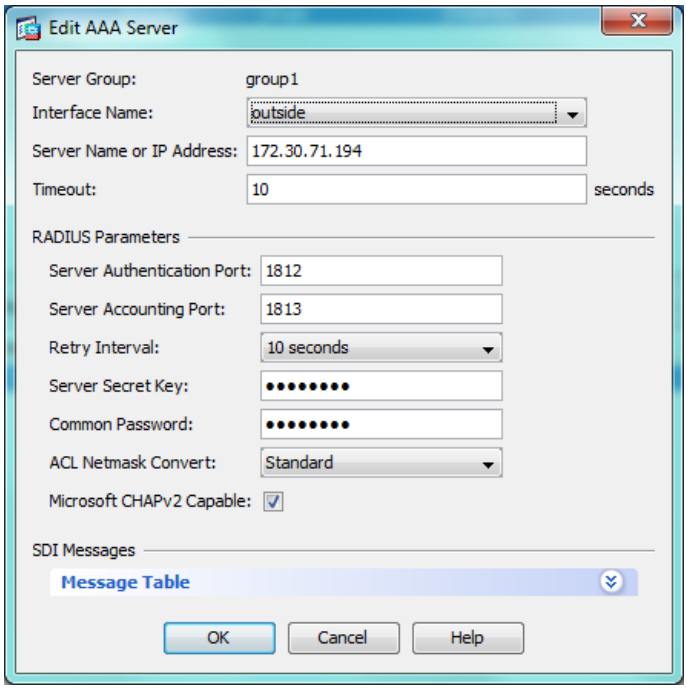
Under *AAA Server Groups* select *Add*.

Create a group that the FortiAuthenticator device will later be added to as shown and select *OK*.



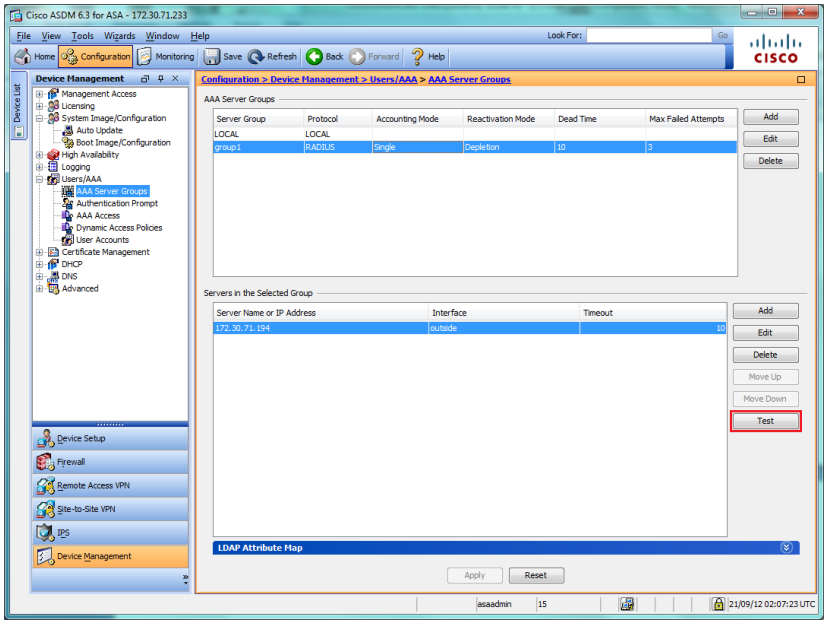
Select the *Server Group* specified in the previous step and, in the *Servers in Selected Group* window, click Add.

Specify the details of the FortiAuthenticator device as shown, taking care to include the correct *Pre-Shared Key* (Server Secret Key)



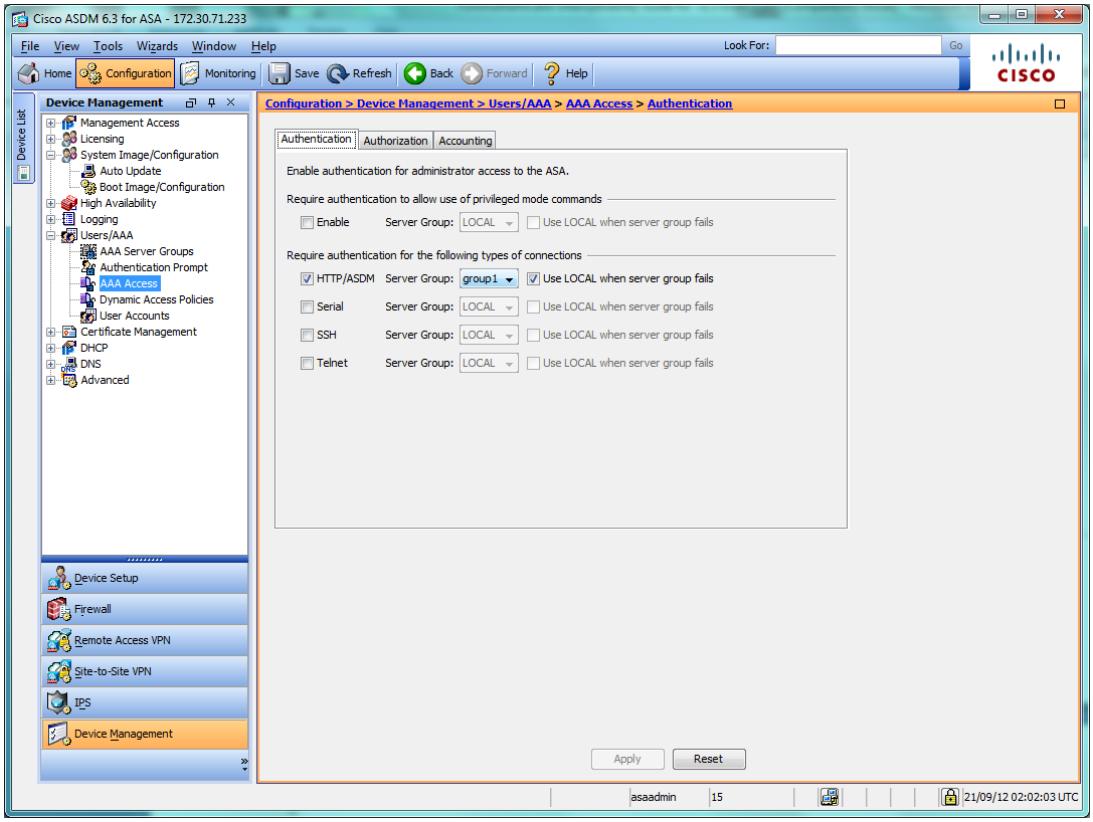
Once complete, select *OK*.

The configuration can be validated by selecting the group and the FortiAuthenticator server and selecting *Test*.



To configure authentication of the Cisco ASA system via FortiAuthenticator two-factor authentication:

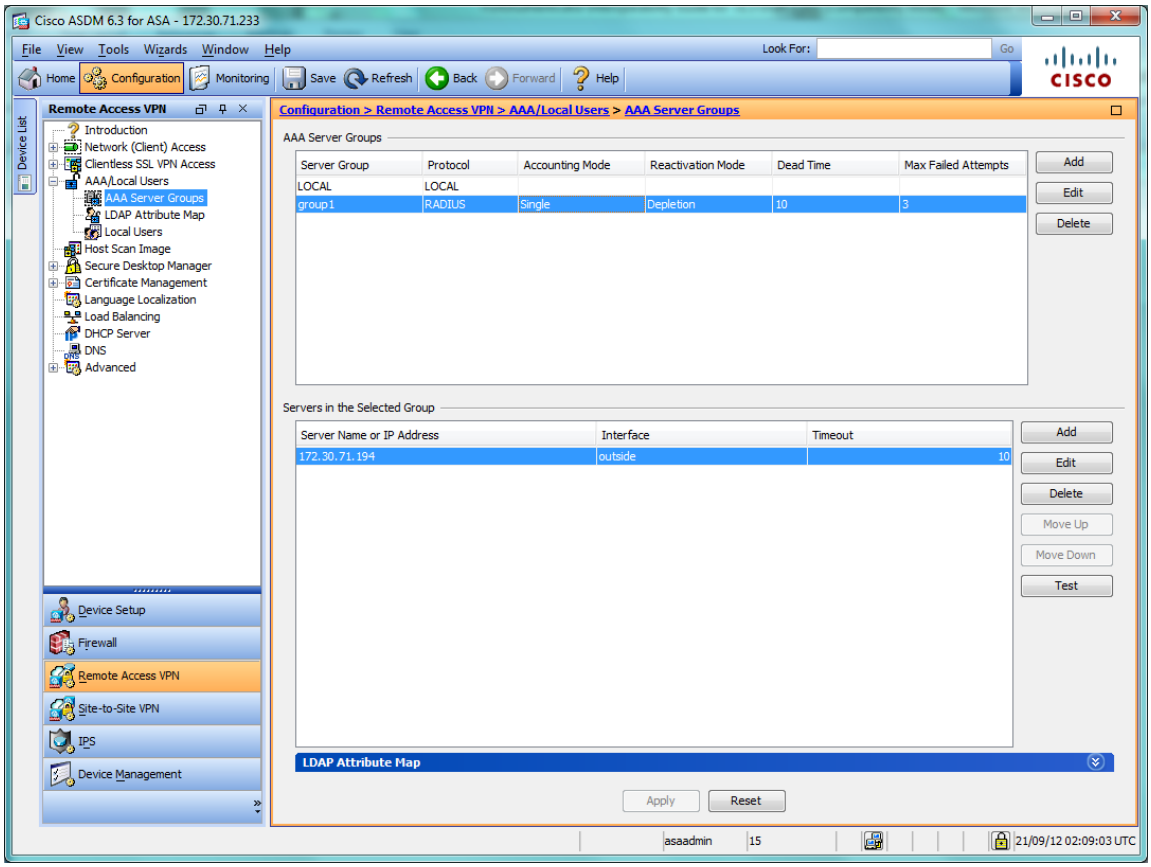
1. Go to *Device Management* > *Users/AAA* > *AAA Access*.
2. In the *Authentication* tab, under *Require authentication for the following types of connection*, select the mode you wish to employ FortiAuthenticator two-factor authentication to, e.g. *HTTP/ASDM Management* as shown.



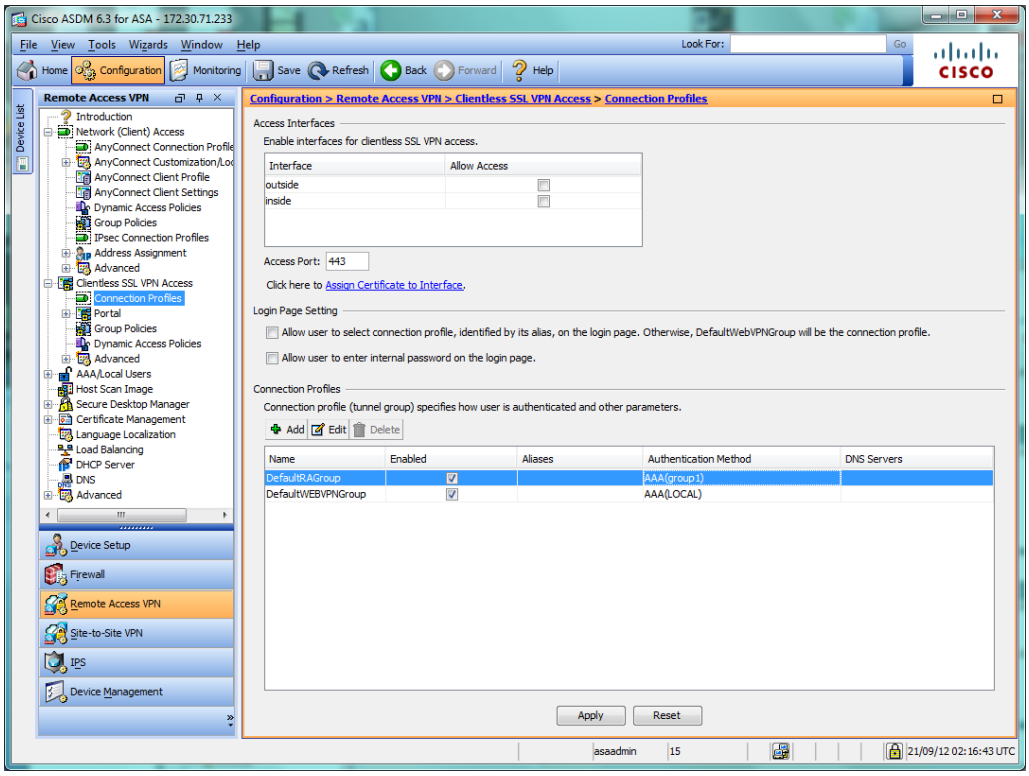
Configuring Remote Access Authentication

To configure authentication for Remote Access VPN, the configuration from the previous step is repeated.

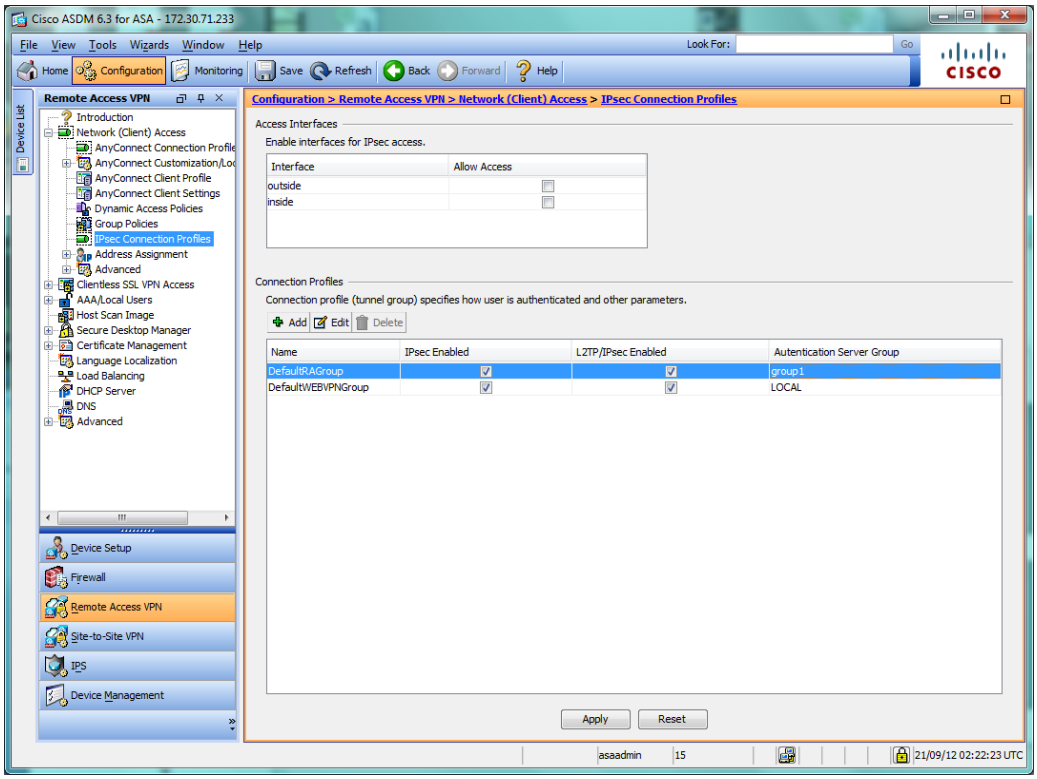
1. In *Remote Access VPN* > *AAA/Local Users* > *AAA Server Groups*, select *Add* and create a group.
2. Create a server and add the server to the group.



To enable two-factor authentication with FortiAuthenticator on the SSL-VPN, go to *Remote Access-VPN* > *Clientless SSL VPN Access* > *Connection Profiles* and set the required group members to the *Authentication Method (RADIUS)* and group created in the previous step.



To enable two-factor authentication with FortiAuthenticator on the IPSEC VPN, go to *Remote Access-VPN* > *Network (Client) Access* > *IPSEC Connection Profiles* and set the required group members to the Authentication Method (RADIUS) and Group created in the previous step.

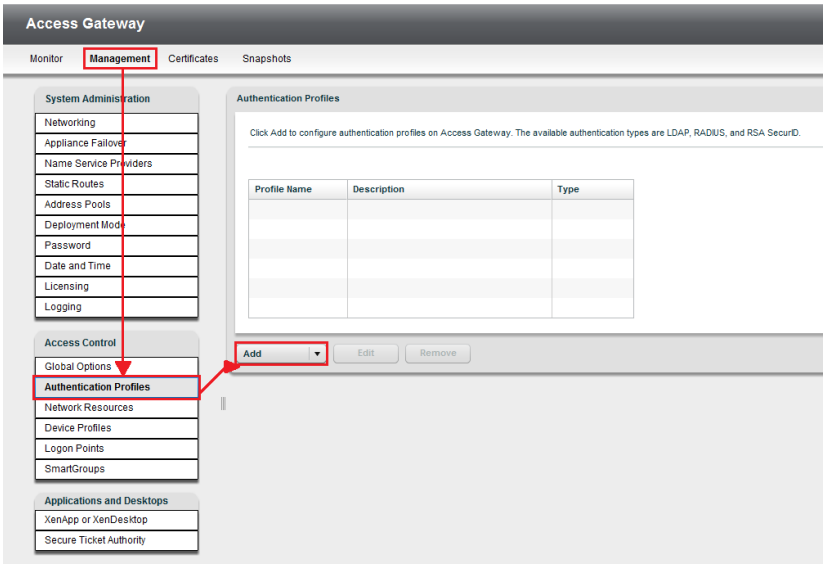

Cisco ASDM 6.3 for ASA - 172.30.71.233
File View Tools Wizards Window Help
Look For:
Home Configuration Monitoring Save Refresh Back Forward Help
Remote Access VPN
Introduction
Network (Client) Access
AnyConnect Connection Profile
AnyConnect Customization/Lo
AnyConnect Client Profile
AnyConnect Client Settings
Dynamic Access Policies
Group Policies
IPsec Connection Profiles
Address Assignment
Advanced
Clientless SSL VPN Access
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
Language Localization
Load Balancing
DHCP Server
DNS
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
IPS
Device Management
Configuration > Remote Access VPN > Network (Client) Access > IPsec Connection Profiles
Access Interfaces
Enable interfaces for IPsec access.
Interface
Allow Access
outside
inside
Connection Profiles
Connection profile (tunnel group) specifies how user is authenticated and other parameters.
Add Edit Delete
Name
IPsec Enabled
L2TP/IPsec Enabled
Autentication Server Group
DefaultRAGroup
group1
DefaultWEBVPNGroup
LOCAL
Apply
Reset
asaadmin
15
21/09/12 02:22:23 UTC

Citrix Access Gateway

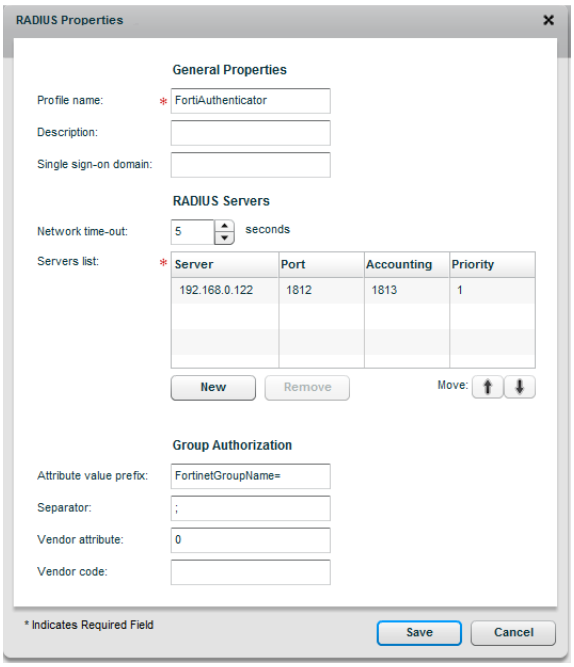
Before proceeding, ensure that you have followed the steps detailed in Chapter titled "Basic Configuration" on page 7. Pay particular attention to "Create test user" on page 11 and ensure you have created a NAS entry for the device you will be testing otherwise all authentication attempts will be ignored for security reasons.

Configure the RADIUS Server

Log into the Citrix Access Gateway Management GUI *https://<Management_IP/lp/adminlogonpoint*, go to *Management Access → Control → Authentication Profiles* and select *Add*.



Enter the details of the remote FortiAuthenticator including the *IP Address* and *shared secret*, and select *Save*.

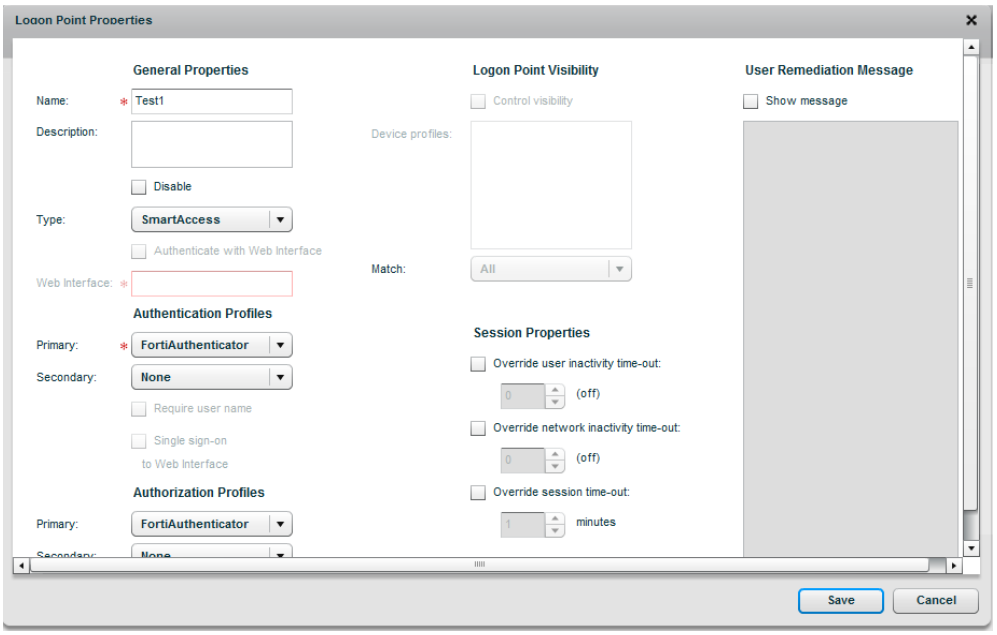


Create a logon point

A logon point in Citrix Access Gateway is the URL to which the user logs on to access a protected resource. In this example, a test Logon Point is created but the same detail can be used to modify an existing Logon Point.

Go to *Access Control* > *Logon Points* and select *New*.

Create a Test logon point, e.g. *Test1* with *Type* set to *SmartAccess*. Select the FortiAuthenticator as the *Primary* authentication profile as created in the previous section. Optionally configure an authorization profile using the same FortiAuthenticator settings, and select *Save*.



User logon to the Citrix Access Gateway

There are two options for FortiAuthenticator authenticated logon to the Citrix Access Gateway: *Token Appended* and *Challenge-Response*.

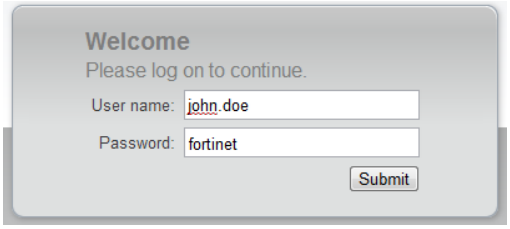
Challenge-Response is the most simple method for users and is shown below.

Attempt to log into the Citrix Access Gateway User GUI with the user credentials from the FortiAuthenticator. The *Username* and *Password* can be entered without the token PIN e.g.

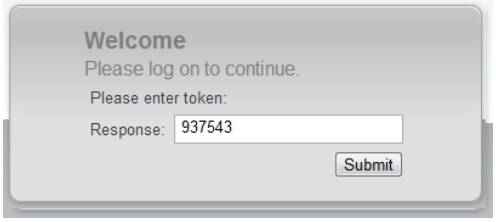
Username: `john.doe`

Password: `<password>`

For example, if the password was *fortinet* and the one-time PIN was *937543*, the login would become

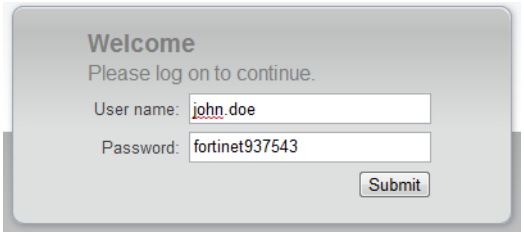


The FortiAuthenticator detects the missing token PIN and sends a RADIUS challenge which the Citrix Access Gateway presents to the user.



Successful authentication will provide the user with access to the Citrix Access Gateway resource.

As an alternative a single step login can be made to bypass the challenge using the token appended method, e.g.



Successful authentication will provide the user with access to the Citrix Access Gateway resource and will generate a login event in *Monitor* > *Audit*.

```
192.168.0.254 - 0xb0409002a18b9b1:john.doe\:Test1:
[04/Apr/2012:06:08:41 -0700] "" - - "" "" Login "NavUI"
```

If authentication is unsuccessful, follow the steps in Appendix A – Debugging to identify what is wrong.

F5 Big-IP

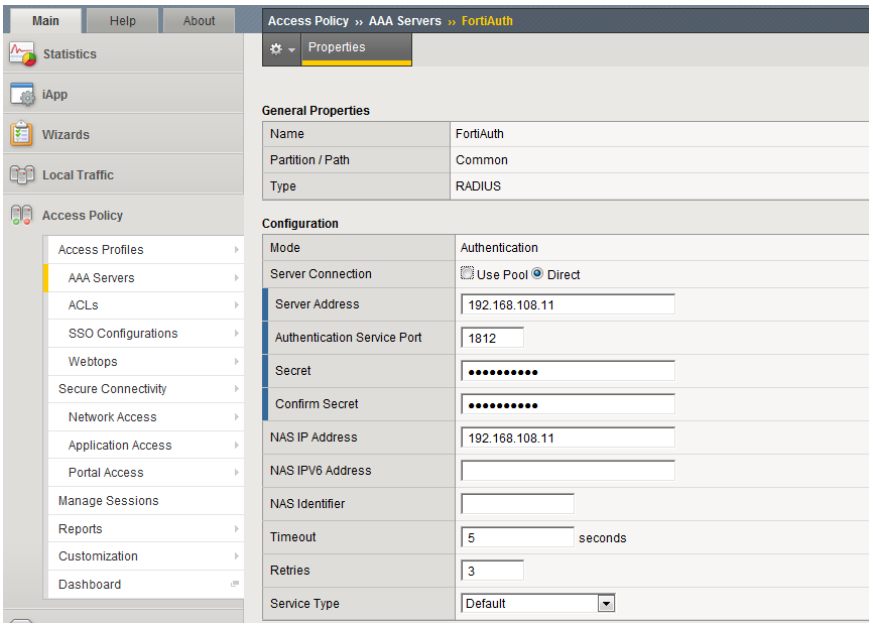
Before proceeding, ensure that you have followed the steps detailed in Chapter titled "Basic Configuration" on page 7. Pay particular attention to "Create test user" on page 11 and ensure you have created a NAS entry for the device you will be testing otherwise all authentication attempts will be ignored for security reasons.

The following configuration was performed on an F5 Big-IP Edge Gateway device however, given the shared OS, this configuration should also be transferable to other devices in the Big-IP range including Local Traffic Manager (LTM).

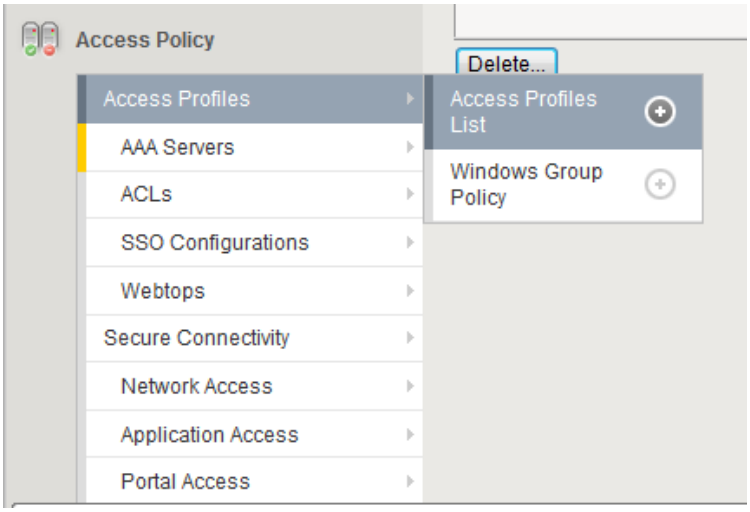
Configure the AAA Server

Log into the F5 Big-IP device and browse to *Main* > *Access Policy* > *AAA Servers* > *RADIUS* and select the + symbol to add a new configuration.

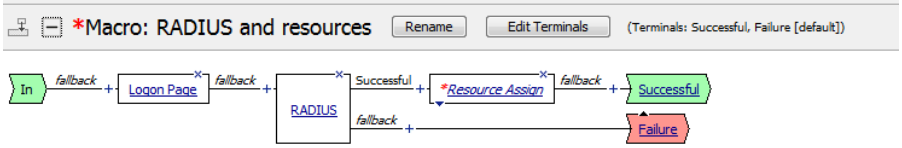
Enter the details of the FortiAuthenticator including IP (Server) Address, port, and secret.



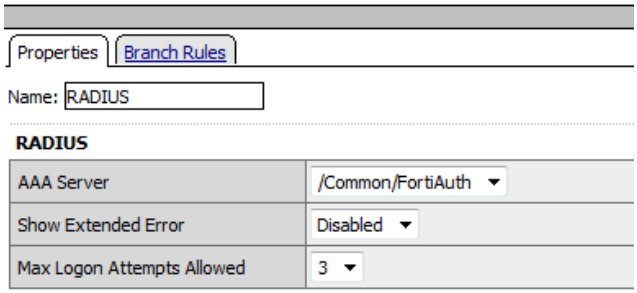
Next go to *Main* > *Access Policy* > *Access Profiles* > *Access Profiles List* and select the + symbol to add a new configuration.



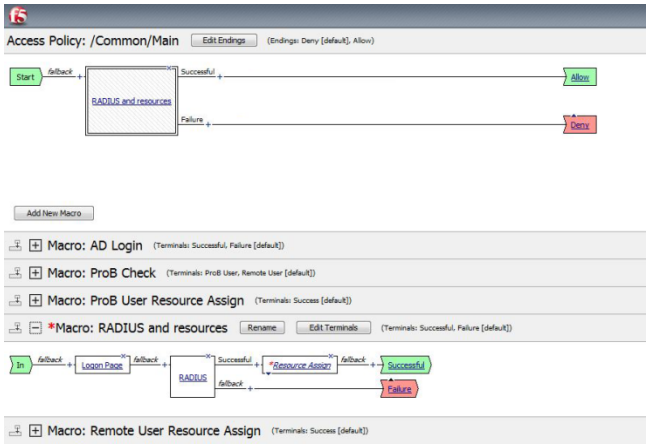
Create a RADIUS resource profile (see the F5 documentation for detailed explainations of this section). This profile binds the RADIUS authentication method to the Logon Page and defines what happens on successful or unsuccessful authentication.



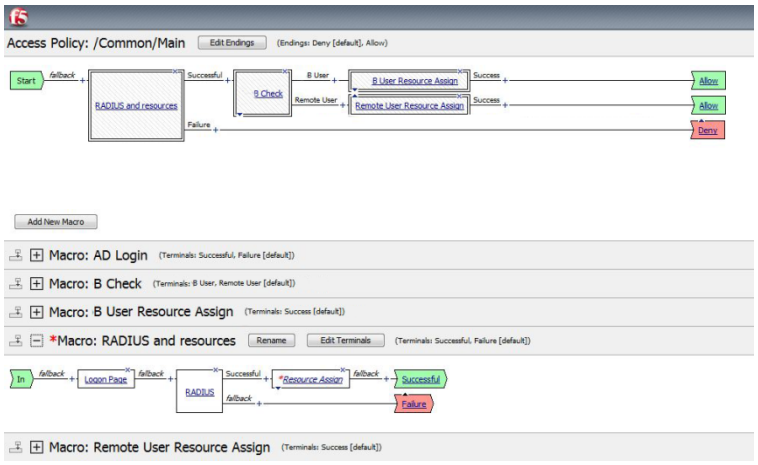
Edit the RADIUS object and define the correct details for the FortiAuthenticator as created in the previous Access Policy step (Server defined as FortiAuth). Note that extended errors may be useful for debugging but should be disabled during normal operation.



Once the RADIUS Authentication method has been defined, it should be configured for use in the Main Access Policy.



Additional validation steps can be defined if required.



Subsequent attempts to authenticate with token enabled users will result in an additional challenge prompting for the token.

User logon to the F5 Big-IP Management interface

There are two options for FortiAuthenticator authenticated logon to the F5 Big-IP device: *Token Appended* and *Challenge-Response*.

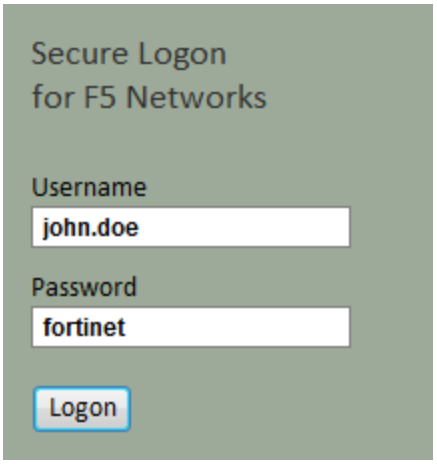
Challenge-Response is the most simple method for users and is shown below.

Attempt to log into the F5 Big-IP User GUI with the user credentials from the FortiAuthenticator. The *Username* and *Password* can be entered without the token PIN, e.g.

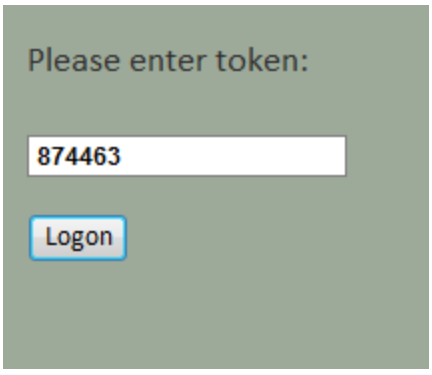
Username: `john.doe`

Password: `<password>`

For example, if the password was *fortinet* and the one-time PIN was *874463*, the login would become

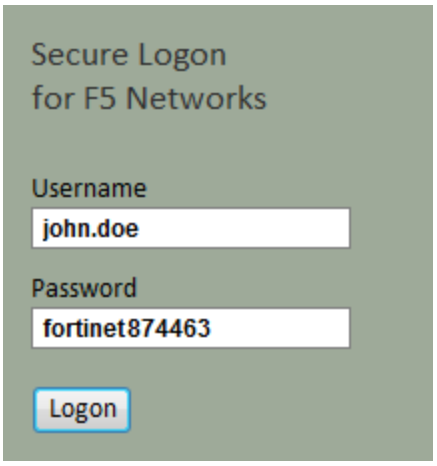


However obviously the password would be starred out. The FortiAuthenticator detects the missing token PIN and sends a RADIUS challenge which the F5 Big-IP presents to the user



Successful authentication will provide the user with access to the F5 Big-IP resource.

As an alternative a single step login can be made to bypass the challenge using the token appended method e.g.



If authentication is unsuccessful, follow the steps in the Chapter Debugging Authentication to identify what is wrong.

Linux Login

Linux uses Pluggable Authentication Modules (PAM) to extend the usual local authentication methods out to external third party devices.

This makes Linux is very flexible in how it can be integrated with two-factor authentication. Applications can be configured so that locally accessed services can be authenticated via password only whilst applications accessible over the Internet can be authenticated using strong two-factor methods.

The instructions below are for Ubuntu 11.04 however, PAM is pretty standard across all Linux distributions so the instructions should be usable with only minor changes.

Integrating Linux with RADIUS (FortiAuthenticator)

In order to integrate with RADIUS authentication and therefore FortiAuthenticator, first you must install the PAM RADIUS Module.

```
$ sudo apt-get install libpam-radius-auth
```

Once installed, edit */etc/pam_radius_auth.conf*. The default configuration will contain the following examples (commented out):

```
#127.0.0.1      secret             1#other-server    other-secret       3
```

To configure the FortiAuthenticator, add an additional line of the format.

```
<FortiAuthenticator Name / IP>   <RADIUS Shared secret>   <Timeout>
```

e.g.

```
192.168.0.110       fortinet    3
```

To configure the FortiAuthenticator, add an additional line of the format.

Enabling Strong Authentication for SSH

Before configuring, make sure that the user you are trying to authenticate already exists on the Linux system. This limitation will be covered in a later section.

To enable two factor authentication in SSH by editing the file /etc/pam.d/ssh and insert the following lines in before the line # Standard Un*x authentication

```
# Enable Two-Factor Authentication with FortiAuthenticatorauth
sufficient     pam_radius_auth.so         debug
```

Note that the debug option at the end of the line increases debugging sent to /var/log/auth.log and can be removed once successfully configured.

Attempt to log into SSH using your chosen client with your new credentials. The Username and Password used to authenticate will include the 6-digit two-factor authentication PIN from your token:

Username: `john.doe`

Password: `<password><Token PIN>`

For example, if the password was *fortinet* and the one-time PIN was *947826*, the login would become

```
login as: john.doe
Password: fortinet947826
Welcome to Ubuntu 11.04 (GNU/Linux 2.6.38-10-generic i686)
Last login: Mon Aug 22 18:09:18 2011 from 192.168.0.24
john.doe@Scooter:~$
```

Successful authentication will provide the user with access to the system via SSH and will generate a login event log on the FortiAuthenticator

ID	Timestamp	Level	Category	Sub Category	Type Id	Short Message	User
193	Mon Aug 22 09:55:11 2011	information	Event	Authentication	20002	RADIUS:Authentication successful with FortiToken	john.doe

If authentication is unsuccessful, follow the steps in Appendix A – Debugging to identify what is wrong.

Enabling Challenge-Response

The configuration described above requires the user to log in with the RADIUS username and password appended with the PIN. The benefit of this is that it supports almost any system which can authenticate with RADIUS. However, the FortiAuthenticator also supports a challenge-response mechanism. When the platform detects that only the password has been returned, it will respond with a RADIUS Challenge-Response and expect the PIN to be returned. This requires the client to support this additional step which the OpenSSH server does.

To configure this step on the SSH Server, edit /etc/ssh/sshd_config and change

```
ChallengeResponseAuthentication no
```

to

```
ChallengeResponseAuthentication yes
```

Restart the SSH Server to apply the setting

```
$ sudo restart ssh
```

Apache Web Server

This document details how to enable RADIUS authentication in Apache2 for use with FortiAuthenticator two-factor authentication. If Apache2 is not installed, install it with

```
sudo apt-get install apache2
```

The Ubuntu 11.04 build of Apache2 comes with the mod-auth-radius module installed and enabled, however, if you need to manually install it

```
sudo apt-get install libapache2-mod-auth-radius
```

and enable it with

```
a2enmod auth_radius
```

At this point, confirm that you can browse to the Apache2 server via http://localhost/ or via the IP/FQDN of your test server.

Modifying the Apache configuration

There is a great deal of documentation on the Internet recommending where to place the relevant configuration lines about to be described. However the majority of this does not appear to work with the current installation of Apache2 on Ubuntu 11.04.

The majority of documentation recommends that the RADIUS server configuration is put into /etc/apache2/apache2.conf or /etc/apache2/httpd.conf however, this does not work and generates an error in the /var/log/apache2/error.log.

```
[warn] AuthRadiusActive set, but no RADIUS server IP - missing AddRadiusAuth
in this context?
```

The following has been tested and confirmed to work correctly.

Edit the default site /etc/apache2/sites-enabled/000-default, or your specific server site if this is configured, adding the lines shown in bold in the positions specified:

```
<VirtualHost *:80>
  ServerAdmin webmaster@localhost
  AddRadiusAuth 192.168.0.110:1812 fortinet 5:3
  AddRadiusCookieValid 5
  DocumentRoot /var/www
  <Directory />
     Options FollowSymLinks
     AllowOverride None
     AuthType Basic
```

```
        AuthName "FortiAuthenticator Secure Authentication"
        AuthBasicAuthoritative Off
        AuthBasicProvider radius
        AuthRadiusAuthoritative on
        AuthRadiusActive On
        Require valid-user
    </Directory>
    <Directory /var/www/>
        Options Indexes FollowSymLinks MultiViews
        AllowOverride None
        Order allow,deny
        allow from all
</Directory>
```

When completed, restart the Apache2 daemon

```
sudo /etc/init.d/apache2 restart
```

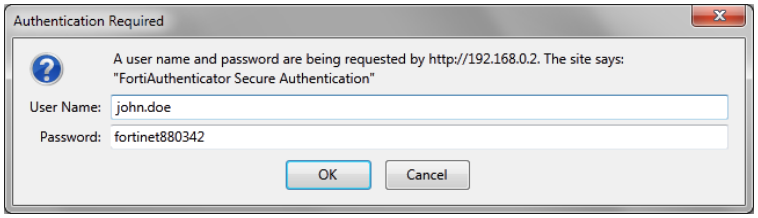
Clear the cache on your browser and restart to avoid any locally cached content from being displayed without the need for authentication.

Browse to the web site configured, e.g. http://localhost/ and you should be prompted for your credentials. The *Username* and *Password* used to authenticate will include the 6-digit two-factor authentication PIN from your token:

Username: `john.doe`

Password: `<password><Token PIN>`

For example, if the password was *fortinet* and the one-time PIN was *880342*, the login would become



Successful authentication will provide the user with access to the page and will generate a login event log on the FortiAuthenticator.

ID	Timestamp	Level	Category	Sub Category	Type Id	Short Message	User
193	Mon Aug 22 09:55:11 2011	information	Event	Authentication	20002	RADIUS:Authentication successful with FortiToken	john.doe

If authentication is unsuccessful, follow the steps in the Chapter Debugging Authentication to identify what is wrong. Additional debugging can be performed using the Apache2 logs located in /var/log/apache2. Most useful is the error.log which will display a log if the RADIUS server credentials are incorrectly configured.

Appendix A – Debugging

FortiAuthenticator is simple to get working however, should you encounter difficulty, there are some simple steps which can be taken to diagnose the problem.

Logging

If authentication is failing on your NAS, the first place to check to see why is the FortiAuthenticator log files.

Bad Password

Try resetting the password if the user insists they have the correct credentials.

276	Tue Aug 23 11:37:04 2011	information	Event	Authentication	20102	RADIUS:Authentication failed, bad password	john.doe

If this persists, verify that the pre-shared secret is correct on both the NAS and the FortiAuthenticator.

Bad Token Code

This may be due to user error (entering the incorrect Token) or may be caused by time issues.

277	Tue Aug 23 11:38:16 2011	information	Event	Authentication	20103	RADIUS:Authentication failed, bad token code	john.doe

To debug this issue, verify the following:

- Ensure the user is not trying to use a previously used Token number. i.e. you cannot log in twice with the same Token number.
- The time and time zone on the FortiAuthenticator is correct and preferably synchronised using NTP.
- The Token is correctly synced with the FortiAuthenticator. Verify the drift by syncing the token as shown in Section.

Nothing Logged

If there is no failure or successful authentication logged. This will be generally be due to one of two things:

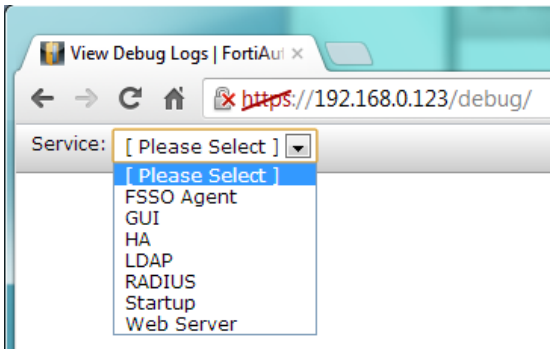
1. Request is not reaching the FortiAuthenticator. Verify that any intervening firewalls are permitting the required traffic through the network. RADIUS Authentication traffic will require UDP Port 1812 opening to the FortiAuthenticator and pseudo-stateful responses allowed to return.
2. Request is reaching the FortiAuthenticator but is being ignored. If traffic is seen reaching the FAC (e.g. by packet sniffing) but is being ignored, it is most likely that the requesting NAS not configured in the FortiAuthenticator. Verify that the NAS is sending the traffic from the expected IP and not from a secondary IP or alternative interface. The FortiAuthenticator RADIUS server will not respond to requests from an unknown NAS for security reasons.

   One other less likely possibility is the NAS_Calling_IP Attribute is set to an incorrect value.

Extended Logging

The standard GUI Logs found *Logging* > *Log Access* > *Logs* provide a concise summary of events occurring on the system, particularly the information needed for audit purposes (who logged in, when, and where from). However there are times when a more detailed view is required in order to debug issues.

Detailed system and application logs can be found by browsing to *https://<FAC_IP>/debug/*.

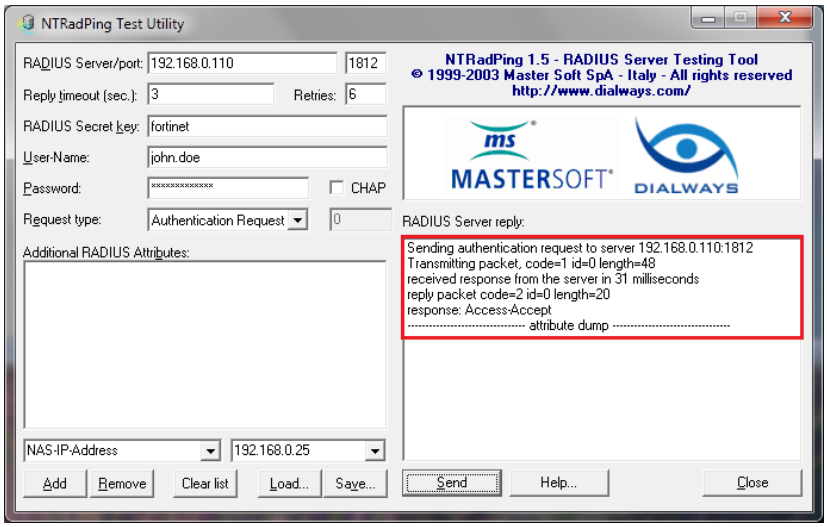


There are several log files as detailed below:

FSSO Agent	Details of Fortinet Single Sign-On events.
GUI	Errors encountered whilst rendering the appliance GUI.
HA	Details of and errors in the HA process.
LDAP	Details of the LDAP authentication process for both local and remote connections.
RADIUS	Details of the RADIUS authentication process.
Startup	Errors during creation of the initial database and during the system startup.
Web Server	Errors encountered by the WebServer.

RADIUS Packet Generation

Testing authentication directly without the use of a NAS device is useful to rule out issues with the NAS device. This is most easily achieved by using a tool such as NTRADPing.


NTRadPing Test Utility
RADIUS Server/port: 192.168.0.110 1812
Reply timeout (sec.): 3 Retries: 6
RADIUS Secret key: fortinet
User-Name: john.doe
Password: ********** CHAP
Request type: Authentication Request 0
Additional RADIUS Attributes:
NAS-IP-Address 192.168.0.25
Add Remove Clear list Load... Save...
NTRadPing 1.5 - RADIUS Server Testing Tool
© 1999-2003 Master Soft SpA - Italy - All rights reserved
http://www.dialways.com/
MASTERSOFT
DIALWAYS
RADIUS Server reply:
Sending authentication request to server 192.168.0.110:1812
Transmitting packet, code=1 id=0 length=48
received response from the server in 31 milliseconds
reply packet code=2 id=0 length=20
response: Access-Accept
---------- attribute dump ----------
Send Help... Close

Appendix B – Supported Two-Factor Authentication Methods

Product	Feature	FortiToken Direct	FortiAuthenticator (Token Appended)	FortiAuthenticator (Token Challenge)	Wildcard Users
FortiGate 5.0	**NAT Route Mode**				
tested on FortiGate 5.0 PR4 and ForrtiClient 5.0.4	Web Based Management	✔	✔	✔	✔ [1]
	SSH Based Management	✔	✔	✔	✔
	Telnet Management	✔	✔	✔	✔
	IPsec VPN (FortiClient)	✔	✔	✔	✔
	SSL VPN (Web)	✔	✔	✔	✔
	SSL VPN (FortiClient)	✔	✔	✔	✔
	Identity Based Policy	✔	✔	✔	✔
	Web Filtering Override	x	✔	x	✔
	Explicit Proxy				
	Identity Based Policy (Basic Auth)	x	✔	x	x
	Identity Based Policy (Forms Auth)	x	✔	x	x
	Web Filtering Override	x	✔	x	x

Product	Feature	FortiToken Direct	FortiAuthenticator (Token Appended)	FortiAuthenticator (Token Challenge)	Wildcard Users
FortiManager tested on FortiManager 5.0.4	Web Based Management	x	✔	x	✔
	SSH Based Management	x	✔	x	✔
	Telnet Management	x	✔	x	✔
FortiAnalyzer tested on FortiAnalyzer 4.0 MR3 PR1	Web Based Management	x	✔	x	x
	SSH Based Management	x	✔	x	x
	Telnet Management	x	✔	x	x
FortiMail tested on FortiMail 4.0 MR3 GA	Web Based Management	x	✔	x	x
	SSH Based Management	x	✔	x	x
	Telnet Management	x	✔	x	x
FortiWeb tested on FortiWeb 4.0 MR3 PR6	Web Based Management	x	✔	x	x
	SSH Based Management	x	✔	x	x
	Telnet Management	x	✔	x	x
Citrix Access Gateway tested on Citrix Access Gateway 5.0	Web Based Management	x	✔	✔	✔
	SSH Based Management	x	✔	✔	✔
	Web Based User Authentication	x	✔	✔	✔

Product	Feature	FortiToken Direct	FortiAuthenticator (Token Appended)	FortiAuthenticator (Token Challenge)	Wildcard Users
Cisco ASA tested on Cisco ASA 8.2(1)	Web Based Management	x	✔	✔	✔
	SSH Based Management	x	✔	✔	✔
	SSL-VPN	x	✔	✔	✔
	IPsec VPN	x	✔	✔	✔
F5 BIG-IP EG tested on TMOS 11.2.1	Web Based Management	x	✔	✔	✔
	SSH Based Management	x	✔	✔	✔
SSH tested on OpenSSH version 5.8p1	SSH Login	x	✔	✔	✔
Apache tested on Apache 2.2.17	Web Authentication	x	✔	✔	✔
Tested with FortiAuthenticator 3.0 GA [1] Mantis 02 22003: Wildcard supported but only with Token Appended					

Appendix C – Syncing FortiTokens

Under most circumstances, it is not necessary to synchronize a FortiToken unless the time on the host FortiAuthenticator system has been allowed to deviate from the correct time. It is essential that the time is kept accurate at all times to prevent issues occurring so configuration of an NTP server is recommended.

Under normal operation, the natural drift of the time on the FortiToken (as found in all clocks) is accounted for automatically by the FortiAuthenticator. Every time a user logs in, the FortiAuthenticator calculates the drift and if it is within +/- 1 (where 1 is a token cycle of 60 seconds), the drift is adjusted accordingly. Should the drift deviate by greater than 1 (i.e. the clock is more than 60 seconds out) since the last login, a manual synchronization is required.

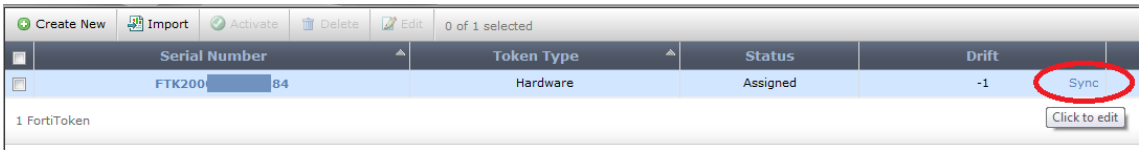
If this is required for several tokens, it is an indicator that the time may be inaccurate on the FortiAuthenticator. Verify the current time and the NTP settings.

Administrator Synchronization

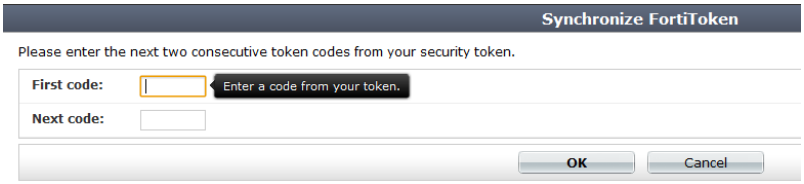
It is possible for the administrator to synchronize a token for use on the FortiAuthenticator and sometime advisable when issuing new tokens which have been held in storage for an extended period or are being reissued.

If this is required for several tokens, it is an indicator that the time may be inaccurate on the FortiAuthenticator. Verify the current time and the NTP settings.

Go to *Authentication* > *FortiTokens* and mouse-over the required token drift category. An option to sync will appear.



Select *Sync* and follow instructions to input two consecutive Token PINs.



Key points to note during the synchronization process are:

- Ensure that the FortiAuthenticator time is accurate before proceeding.
- Ensure the serial of the token you are trying to synchronize matches that on the reverse of the token.
- Ensure that the token has not been used in the preceding 60 seconds. All tokens are one time passwords and cannot therefore be used to authenticate (successful or otherwise) and synchronize.
- Once successfully synchronized, wait a further 60 seconds before attempting to log in. A token used to synchronize cannot be re-used to authenticate.

User Synchronization

Should it be required, FortiAuthenticator provides a mechanism for the user to perform their own manual synchronization. The user should be allowed to access the FortiAuthenticator WebUI, e.g https:/<FAC_IP>/login/.

On logging into the FortiAuthenticator the user will be prompted to enter their token PIN. If the token PIN is out of sync, they will be prompted to enter two consecutive PINs. If the user receives no such prompt, the token is already correctly synchronized.